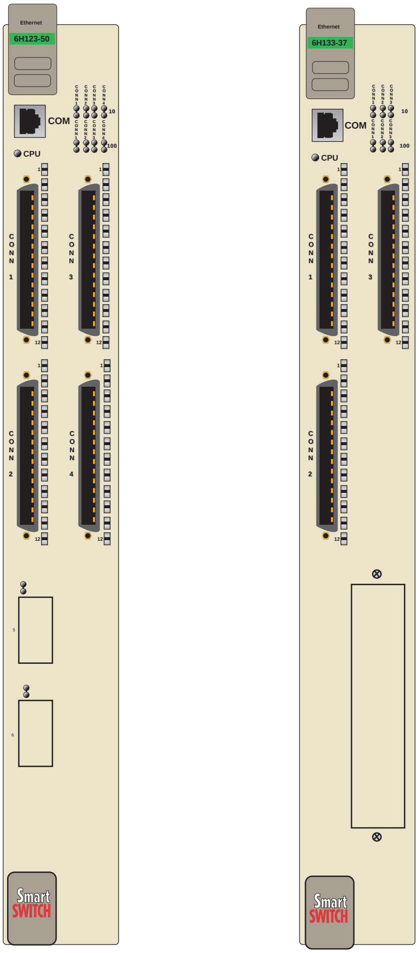
6H123-50 and 6H133-37 MicroLAN SmartSwitch 6000 Interface Modules User's Guide



9032276-04

CABLETRON SYSTEMS

Only qualified personnel should perform installation procedures.

NOTICE

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Order Number: 9032276-04 September 1998

Cabletron Systems, **SPECTRUM**, **LANVIEW**, **QuickSET**, **SecureFast**, and **BRIM** are registered trademarks and **SecureFast Switching** and **SmartSwitch** are trademarks of Cabletron Systems, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator’s manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Printed on ♻ Recycled Paper

INDUSTRY CANADA NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI NOTICE

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

　この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CABLETRON SOFTWARE PROGRAM LICENSE

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

   You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

EXCLUSION OF WARRANTY AND DISCLAIMER OF LIABILITY

1. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

   CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

2. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR ON THE DURATION OR LIMITATION OF IMPLIED WARRANTIES, IN SOME INSTANCES THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

UNITED STATES GOVERNMENT RESTRICTED RIGHTS

The enclosed product (a) was developed solely at private expense; (b) contains “restricted computer software” submitted with restricted rights in accordance with Section 52227-19 (a) through (d) of the Commercial Computer Software - Restricted Rights Clause and its successors, and (c) in all respects is proprietary data belonging to Cabletron and/or its suppliers.

For Department of Defense units, the product is licensed with “Restricted Rights” as defined in the DoD Supplement to the Federal Acquisition Regulations, Section 52.227-7013 (c) (1) (ii) and its successors, and use, duplication, disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

SAFETY INFORMATION

CLASS 1 LASER TRANSCEIVERS

THE FE-100F3 FAST ETHERNET INTERFACE MODULE, FPIM-05 AND FPIM-07 FDDI PORT INTERFACE MODULES, AND APIM-29 ATM PORT INTERFACE MODULE USE CLASS 1 LASER TRANSCEIVERS. READ THE FOLLOWING SAFETY INFORMATION BEFORE INSTALLING OR OPERATING THESE MODULES.

The Class 1 laser transceivers use an optical feedback loop to maintain Class 1 operation limits. This control loop eliminates the need for maintenance checks or adjustments. The output is factory set, and does not allow any user adjustment. Class 1 Laser transceivers comply with the following safety standards:

- 21 CFR 1040.10 and 1040.11 U.S. Department of Health and Human Services (FDA).
- IEC Publication 825 (International Electrotechnical Commission).
- CENELEC EN 60825 (European Committee for Electrotechnical Standardization).

When operating within their performance limitations, laser transceiver output meets the Class 1 accessible emission limit of all three standards. Class 1 levels of laser radiation are not considered hazardous.

SAFETY INFORMATION

CLASS 1 LASER TRANSCEIVERS

LASER RADIATION AND CONNECTORS

When the connector is in place, all laser radiation remains within the fiber. The maximum amount of radiant power exiting the fiber (under normal conditions) is -12.6 dBm or 55 x 10^{-6} watts.

Removing the optical connector from the transceiver allows laser radiation to emit directly from the optical port. The maximum radiance from the optical port (under worst case conditions) is 0.8 W cm^{-2} or 8 x 10^{3} W m^{2} sr-1.

Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.

DECLARATION OF CONFORMITY

Application of Council Directive(s):	**89/336/EEC** **73/23/EEC**
Manufacturer's Name:	**Cabletron Systems, Inc.**
Manufacturer's Address:	**35 Industrial Way** **PO Box 5005** **Rochester, NH 03867**
European Representative Name:	**Mr. J. Solari**
European Representative Address:	**Cabletron Systems Limited** **Nexus House, Newbury Business Park** **London Road, Newbury** **Berkshire RG13 2PZ, England**
Conformance to Directive(s)/Product Standards:	**EC Directive 89/336/EEC** **EC Directive 73/23/EEC** **EN 55022** **EN 50082-1** **EN 60950**
Equipment Type/Environment:	**Networking Equipment, for use in a Commercial or Light Industrial Environment.**

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer	Legal Representative in Europe
Mr. Ronald Fotino	Mr. J. Solari
Full Name	Full Name
Principal Compliance Engineer	Managing Director - E.M.E.A.
Title	Title
Rochester, NH, USA	Newbury, Berkshire, England
Location	Location

CONTENTS

CHAPTER 1 INTRODUCTION

CHAPTER 2 NETWORK REQUIREMENTS

CHAPTER 3 INSTALLATION

CHAPTER 4 TROUBLESHOOTING

CHAPTER 5 LOCAL MANAGEMENT

APPENDIX A SPECIFICATIONS

APPENDIX B FE-100TX, FE-100FX AND FE-100F3 SPECIFICATIONS

APPENDIX C OPTIONAL INSTALLATIONS AND MODE SWITCH BANK SETTINGS

INDEX

CHAPTER 1

INTRODUCTION

Welcome to the Cabletron Systems **6H123-50 and 6H133-37 MicroLAN SmartSwitch 6000 Interface Modules User’s Guide**. This guide describes the 6H123-50 and 6H133-37 interface modules and provides information concerning network requirements, installation, troubleshooting, and Local Management.

1.1 USING THIS GUIDE

Read through this guide completely to understand the interface module features, capabilities, and Local Management functions. A general working knowledge of Ethernet and IEEE 802.3 type data communications networks and their physical layer components is helpful when using these devices.

NOTE

Unless noted differently, the information in this guide applies to both SmartSwitch 6000 interface modules, which are referred to as either the “6H123-50 and 6H133-37” or the “modules”.

1.2 STRUCTURE OF THIS GUIDE

This guide is organized as follows:

Chapter 1, **Introduction**, outlines the contents of this manual, describes the features of the 6H123-50 and 6H133-37, provides instructions on obtaining additional help and concludes with a list of related manuals.

Chapter 2, **Network Requirements**, explains the network requirements to consider before installing the 6H123-50 and 6H133-37 into the 6C105 SmartSwitch 6000 chassis.

Chapter 3, **Installation**, provides instructions on how to install the modules in the chassis and connect segments to the devices.

Chapter 4, **Troubleshooting**, details the 6H123-50 and 6H133-37 LANVIEW LEDs that enable you to quickly diagnose network/operational problems.

Chapter 5, **Local Management**, describes accessing Local Management and using the Local Management screens to manage the 6H123-50 and 6H133-37 modules, and the 6C105 chassis.

Appendix A, **Specifications**, contains information on functionality and operating specifications, connector pinouts, environmental requirements, and physical properties.

Appendix B, **FE-100TX, FE-100FX and FE-100F3 Specifications**, contains information about FE-100TX pinouts and information concerning cable types used with the FE-100FX and FE-100F3.

Appendix C, **Optional Installations and Mode Switch Bank Settings**, describes how to install optional Fast Ethernet Interface Modules and how to set the Mode Switches.

1.3 OVERVIEW

The 6H123-50 and 6H133-37, shown in Figure 1-1, are interface modules for the Cabletron Systems 6C105 SmartSwitch 6000 chassis.

The 6H123-50 and 6H133-37 are high-speed network repeater/switch devices. The 6H123-50 provides four Ethernet repeated segments and four Fast Ethernet repeated segments (CONN 1 through CONN 4). The 6H133-37 provides three Ethernet repeated segments and three Fast Ethernet repeated segments (CONN 1 through CONN 3). The RJ21 connectors each consist of 12 repeater ports that are able to reside on the Ethernet (10 Mbps) or the Fast Ethernet (100 Mbps) segment. Each Ethernet and Fast Ethernet segment supports 802.1D switching (bridging), Cabletron Systems SecureFast Switching Virtual Network technology and IEEE 802.1Q Port Based VLANs.

Slots 5 and 6 (interfaces 9 and 10) of the 6H123-50 support optional Fast Ethernet Interface Modules providing uplinks to 100BASE-TX or 100BASE-FX Fast Ethernet networks. The 6H133-37 is capable of being equipped with a High Speed Interface Module (HSIM) that provides for additional connectivity to other high speed networking technologies such as Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI) and Wide Area Network (WANs).

The 6H123-50 and 6H133-37 switch each Ethernet and Fast Ethernet segment (CONN 1 through CONN 4 and CONN 1 through CONN 3) to one another and to the optional Fast Ethernet Interface modules of the 6H123-50 or an HSIM installed in the 6H133-37.

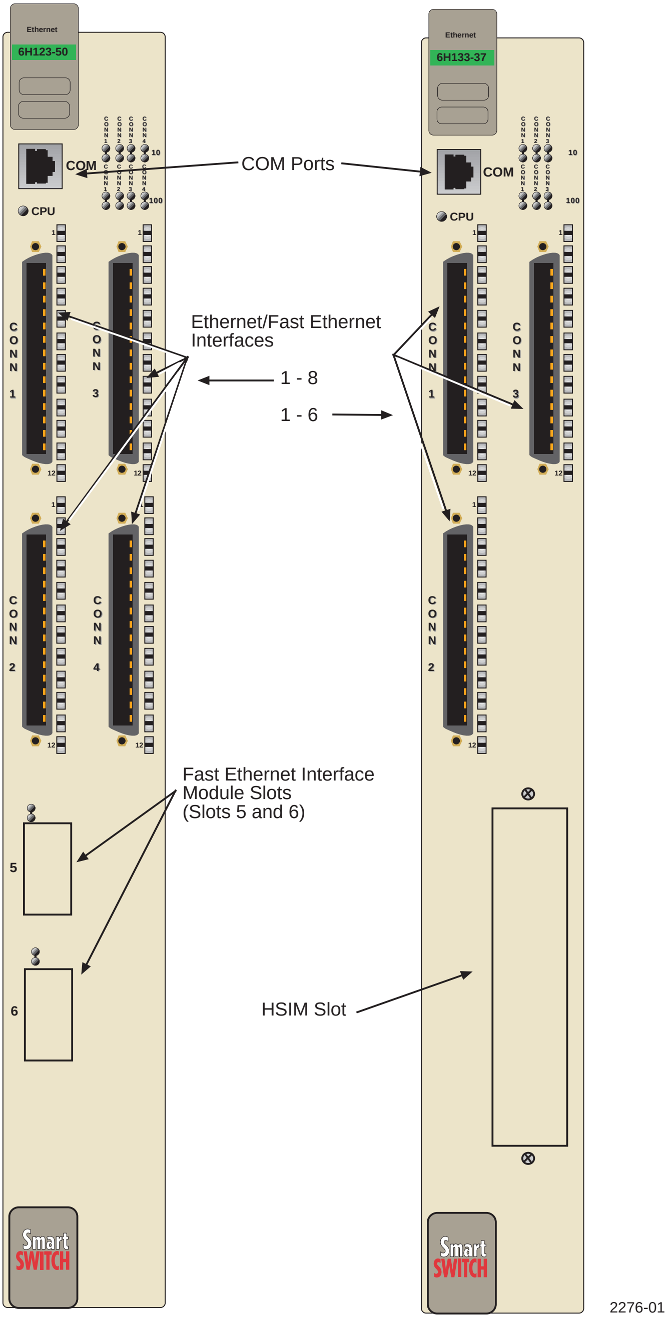


Figure 1-1 The 6H123-50 and 6H133-37

Table 1-1 shows the port organization for both modules.

Table 1-1 Port Organization

6H123-50	6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 4 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	HSIM = Port 7
Fast Ethernet Slot 5 = Port 9	
Fast Ethernet Slot 6 = Port 10	

1.3.1 Connectivity

The 6H123-50 and 6H133-37 connect to Ethernet/Fast Ethernet networks or workstations through RJ21 ports on the front panel. Each port supports a 25-pair cable at lengths up to 100 meters (each pair must be Category 5 compliant with an impedance of 85 to 111 ohms). The ports are IEEE 802.3 10BASE-T and IEEE 802.3u 100BASE-TX compliant.

The 6H123-50 has two front panel slots (connectors 5 and 6 or interfaces 9 and 10) for optional Fast Ethernet Interface Modules to support an uplink to Fast Ethernet backbones or a high speed connection to a local server.

The 6H133-37 has one front panel slot for an optional High Speed Interface Module (Interface 7) to provide for additional connectivity to other high speed networking technologies such as ATM, FDDI, and WANs.

Cables available for 100BASE-TX operation include the following:

- 180° angle connector (straight-through RJ21-to-RJ21)
- 180° RJ21-to-RJ45 connector
- 120° angle connector with the same options

1.3.2 Full Duplex Switched Ethernet

The optional Fast Ethernet Interface Modules for the 6H123-50 can be configured to operate in Full Duplex Switched Ethernet mode, which provides up to 200 Mbps of bandwidth.

1.3.3 Auto-Negotiation

The repeater ports and Fast Ethernet Interface Modules can auto-negotiate the type of connection required to provide a link to another device. During Auto-Negotiation, two devices automatically exchange information “telling” each other what their operating capabilities are. The Auto-Negotiation feature targets the maximum capabilities that can be reached between the two devices. For example, an FE-100TX Fast Ethernet Interface Module in a 6H123-50 can adjust to 100 Mbps when the device on the other end of the connection can also adjust to 100 Mbps. If the device on the other end of the connection can only operate at 10 Mbps, then the FE-100TX simply adjusts to 10 Mbps operation.

When Auto-Negotiation is supported at both ends of a link, the two devices dynamically adjust to full or half duplex operation based on the maximum capability that can be reached between the two devices. If the device connected to the FE-100TX cannot auto-negotiate, the FE-100TX Fast Ethernet Interface Module operates according to the capabilities of the other device.

1.3.4 SmartTrunking

SmartTrunk, also referred to as SmartTrunking, is Cabletron Systems’ terminology for load balancing or load sharing. SmartTrunk technology provides an easy-to-implement mechanism to group, or aggregate, multiple physical links together to scale the backbone bandwidth beyond the limitations of a single link. All links are user-configurable so administrators can scale the backbone bandwidth by adding SmartTrunk links. The SmartTrunk benefits are as follows:

- All purchased bandwidth is used.
- Distributed, resilient links increase reliability and performance.
- Multiple technologies are supported within a single trunk for maximum flexibility.

For more information about SmartTrunk, refer to the Cabletron Systems *SmartTrunk User's Guide*.

1.3.5 Management

Management of the 6H123-50 and 6H133-37 is accomplished using SNMP compliant management tools for in-band Local Management. Out-of-band Local Management is provided through the RJ45 COM port on the front panel using a VT100 terminal or a VT100 terminal emulator. In-band remote management is possible through any SNMP compliant Network Management Software.

Local Management provides the ability to manage the 6H123-50 and 6H133-37 and any of the optional Fast Ethernet Interface Modules installed in slots 5 and 6 of the 6H123-50, or an optional High Speed Interface Module (HSIM) in a 6H133-37.

The associated HSIM user's guide provides detailed information about the HSIM Local Management.

1.3.6 Switching Options

The 6H123-50 and 6H133-37 provide 802.1D switching, 802.1Q switching or SecureFast Switching Virtual Network Services between all of the front panel interfaces including Fast Ethernet Interface Modules installed in a 6H123-50 or an HSIM installed in a 6H133-37.

IEEE 802.1Q switching and SecureFast switching allow for future migration to Virtual Network technologies without requiring the replacement of existing equipment.

1.3.7 Standards Compatibility

The 6H123-50 and 6H133-37 are fully compliant with the IEEE 802.3 standard and the IEEE 802.3u standard. The optional Fast Ethernet Interface Modules are fully compliant with the IEEE 802.3u standard. The 6H123-50 and 6H133-37 provide IEEE 802.1D Spanning Tree Algorithm (STA) support to enhance the overall reliability of the network and protect against "loop" conditions. The 6H123-50 and 6H133-37 support a wide variety of industry standard MIBs including RFC 1213 (MIB II), RFC 1757 (RMON), RFC 1493 (Bridge MIB) and RFC 1354 (FIB MIB). A full suite of Cabletron Systems Enterprise MIBs provide a wide array of statistical information to enhance troubleshooting.

1.3.8 LANVIEW Diagnostic LEDs

LANVIEW diagnostic LEDs serve as an important troubleshooting aid by providing an easy way to observe the status of individual ports and overall network operations. Chapter 4 provides details about the 6H123-50 and 6H133-37 LANVIEW LEDs.

1.3.9 Year 2000 Compliant

These products have an internal clock that can maintain the current time and date beyond the year 1999.

1.3.10 Runtime IP Address Discovery

This feature enables the 6H123-50 and 6H133-37 to automatically accept an IP address from a Boot Strap Protocol (BootP) or Reverse Address Resolution Protocol (RARP) server on the network into NVRAM without requiring a user to enter an IP address through Local Management.

When the 6H123-50 and the 6H133-37 are connected to the network and powered up, Runtime IP Address Discovery (RAD) checks the 6H123-50 and the 6H133-37 for an IP address. If one has not yet been assigned (6H123-50 and 6H133-37 IP address set to 0.0.0.0), RAD checks to see if any of the interfaces have a link. If so, RAD sends out Reverse Address Resolution Protocol (RARP) and BootP requests to obtain an IP address from a BootP server on the network.

The RAD requests start out at an interval of 1 second. The interval then doubles after every transmission until an interval of 300 seconds is reached. At this point, the interval remains at 300 seconds. The RAD requests continue until an IP address is received from a BootP server, or an IP address is entered using Local Management.

1.3.11 Local Management Features

Local Management provides the tools that allow management of the 6H123-50 and 6H133-37, the Fast Ethernet Interface Modules, the High Speed Interface Module (HSIM) and the 6C105 chassis. It also allows the following tasks to be performed:

- Manage any module installed in the 6C105 via a single terminal connection.
- Assign an IP address and subnet mask to the 6H123-50, 6H133-37 and 6C105 chassis.
- Select a default gateway.
- Control local and remote access.
- Designate workstations to receive SNMP traps from the 6H123-50 module, 6H133-37 module, or the 6C105 chassis.
- Configure module specific SNMP MIB objects including the IETF Bridge MIB objects.

Chapter 5 provides detailed information about Local Management of the 6H123-50 and 6H133-37, the optional Fast Ethernet Interface Modules and the 6C105 chassis. The associated High Speed Interface Module user’s guide provides detailed information about Local Management of the applicable HSIM.

1.4 OPTIONAL FEATURES

Options for the 6H123-50 and 6H133-37 are Fast Ethernet Interface Modules and High Speed Interface Modules, which add remote uplink capability.

Cabletron Systems provides Fast Ethernet Interface Modules for the 6H123-50 to support uplinks to 100 Mbps Fast Ethernet backbones or high speed connections to local servers. The Fast Ethernet Interface Modules are listed in Table 1-2.

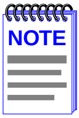
Table 1-2 Fast Ethernet Interface Modules

P/N	Connector	Application
FE-100TX	Uses RJ45 connector	Supports Shielded Twisted Pair (STP), and Category 5 Unshielded Twisted Pair (UTP) cabling, which has an impedance of 85 to 111 ohms.
FE-100FX	Uses SC connector	Supports multimode fiber optic cabling.
FE-100F3	Uses SC connector	Supports single mode fiber optic cabling.

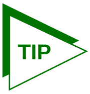
High Speed Interface Modules (HSIMs) are available from Cabletron Systems for the 6H133-37 to provide additional connectivity to other high speed networking technologies such as Asynchronous Transfer Mode (ATM), Wide Area Networks (WANs) and Fiber Distributed Data Interface (FDDI). The HSIMs available for the 6H133-37 are listed in the Release Notes.

1.5 DOCUMENT CONVENTIONS

The following conventions are used throughout this document:



Note symbol. Calls the reader’s attention to any item of information that may be of special importance.



Tip symbol. Conveys helpful hints concerning procedures or actions.

Caution symbol. Contains information essential to avoid damage to the equipment.

Electrical Hazard Warning symbol. Warns against an action that could result in personal injury or death due to an electrical hazard.

1.6 GETTING HELP

For additional support related to this device or document, contact the Cabletron Systems Global Call Center:

World Wide Web	http://www.cabletron.com/
Phone	(603) 332-9400
Internet mail	support@cabletron.com
FTP Login Password	ftp://ftp.cabletron.com/ *anonymous* *your email address*
To send comments or suggestions concerning this document, contact the Cabletron Systems Technical Writing Department via the following email address: **TechWriting@cabletron.com** *Make sure to include the document Part Number in the email message.*	

Before calling the Cabletron Systems Global Call Center, have the following information ready:

- Your Cabletron Systems service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Cabletron Systems products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

1.7 RELATED MANUALS

The following manuals may help to set up, control, and manage the 2H23-50R and 2H33-37R:

Cabletron Systems *HSIM-A6DP User’s Guide*

Cabletron Systems *HSIM-F6 User’s Guide*

Cabletron Systems *HSIM-FE6 User’s Guide*

Cabletron Systems *HSIM-W87 User’s Guide*

Cabletron Systems *HSIM-G01/G09 User’s Guide*

Cabletron Systems *Ethernet Technology Guide*

Cabletron Systems *Cabling Guide*

Cabletron Systems *Port Based VLAN User’s Guide*

Cabletron Systems *SmartTrunk User’s Guide*

These manuals can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

http://www.cabletron.com/

NOTE

All documentation for the Cabletron Systems SecureFast VLAN Manager software is contained on the VLAN Manager CD-ROM.

Documents for the Cabletron Systems HSIM-W6 and HSIM-W84 devices are contained on the QuickSET CD-ROM and are also available on the World Wide Web at: http://www.cabletron.com/

CHAPTER 2
NETWORK REQUIREMENTS

This chapter contains networking guidelines. Before installing and using the 6H123-50 and 6H133-37 or an optional Fast Ethernet Interface Module (FE-100TX, FE-100FX, or FE-100F3), review the requirements and specifications outlined in this chapter concerning the following:

- SmartTrunk (Section 2.1)
- 10BASE-T Twisted Pair Network (Section 2.2)
- 100BASE-TX Twisted Pair Network (Section 2.3)
- 100BASE-FX Fiber Optic Network (Section 2.4)

The network installation must meet the guidelines to ensure satisfactory performance of this equipment. Failure to follow the guidelines may produce poor network performance.

NOTE

The Cabletron Systems *Cabling Guide* and the *SmartTrunk User's Guide*, referred to in the following sections, is located on the Cabletron Systems World Wide Web site: **http://www.cabletron.com/**

2.1 SmartTrunk

To connect the 6H123-50 and 6H133-37 to a network so they can take advantage of the SmartTrunk feature, there are certain rules concerning port connections and configurations that must be followed for proper operation. Refer to the Cabletron Systems *SmartTrunk User's Guide* for additional information.

2.2 10BASE-T NETWORK

When connecting a 10BASE-T segment to any ports of CONN 1 through CONN 4 (6H123-50) or CONN 1 through CONN 3 (6H133-37), ensure that the network meets the IEEE 802.3 Ethernet network requirements for 10BASE-T. Refer to the Cabletron Systems *Cabling Guide* for details.

2.3 100BASE-TX NETWORK

When connecting a 100BASE-T segment to any ports of CONN 1 through CONN 4 (6H123-50), CONN 1 through CONN 3 (6H133-37), or an FE-100TX installed in slot 5 or 6 of the 6H123-50, the device at the other end of the twisted pair segment must meet IEEE 802.3u 100BASE-TX Fast Ethernet network requirements for the devices to operate at 100 Mbps. Refer to the Cabletron Systems *Cabling Guide* for details.

NOTE

The 6H123-50 with an FE-100TX installed is capable of operating at either 10 or 100 Mbps. The FE-100TX can automatically sense the speed of the other device and adjust its speed accordingly.

If operating at 100 Mbps, each pair in a cable must be Category 5 compliant with an impedance of 85 to 111 ohms.

2.4 100BASE-FX FIBER OPTIC NETWORK

Slots 5 and 6 of the 6H123-50 can also support the Cabletron Systems FE-100FX and FE-100F3 fiber optic interface modules. The device at the other end of the fiber optic segment must meet the 100BASE-FX Fast Ethernet network requirements to operate at 100 Mbps. Refer to the Cabletron Systems *Cabling Guide* for details.

Multimode Mode Fiber Optic Cable Length

The maximum multimode fiber optic cable length of a 100BASE-FX segment is covered in the Cabletron Systems *Cabling Guide*.

Single Mode Fiber Cable Lengths

The maximum single mode fiber optic length of a 100BASE-FX segment may be no more than 5 km between Data Terminal Equipment (DTE to DTE) in half duplex mode or 20 km (DTE to DTE) in full duplex mode.

CHAPTER 3

INSTALLATION

Only qualified personnel should install the 6H123-50 and 6H133-37.

This chapter provides the instructions required to install the 6H123-50 and 6H133-37, Follow the order of the sections listed below to ensure a proper installation:

- Required tools (Section 3.1)
- Unpacking the 6H123-50 and 6H133-37 (Section 3.2)
- Installing Options (Section 3.3)
- Installing the 6H123-50 and 6H133-37 in the 6C105 chassis (Section 3.4)
- Connecting to the network (Section 3.5)

3.1 REQUIRED TOOLS

A Phillips screwdriver is required to install the Fast Ethernet Interface Modules in the 6H123-50.

3.2 UNPACKING THE 6H123-50 AND 6H133-37

1. Open the box and remove the packing material protecting the module.
2. Verify the contents of the carton as listed in Table 3-1.

Table 3-1 Contents of 6H123-50 and 6H133-37 Carton

Item	Quantity
6H123-50 or 6H133-37	1
Release Notes	1
Manual Accessory Kit	1

3.3 OPTIONS

NOTE

Install any optional equipment before proceeding to Section 3.4.

If the 6H123-50 will be installed with an optional Fast Ethernet Interface Module, refer to Appendix C for installation instructions. The installation instructions for the HSIMs available for the 6H133-37 are located in the associated user's guide.

3.4 INSTALLING THE 6H123-50 AND 6H133-37 INTO THE 6C105 CHASSIS

CAUTION

Failure to observe static safety precautions could cause damage to the 6H123-50 and 6H133-37. Follow static safety handling rules and properly wear the antistatic wrist strap provided with the 6C105 chassis.

CAUTION

Do not cut the non-conductive bag to remove the module. Damage could result from sharp objects contacting the board or components.

The 6H123-50 and 6H133-37 can be installed in any of the 5 slots that are available in the 6C105. To install a module, proceed as follows:

1. Remove the blank panel covering the slot in which the module is to be installed. All other slots must remain covered to ensure proper airflow and cooling. (Save the blank plate in the event you need to remove the module.)

2. Carefully remove the module from the shipping box. (Save the box and packing materials in the event the module must be reshipped.)

3. Locate the antistatic wrist strap shipped with the 6C105 chassis. Attach the wrist strap to your wrist and plug the cable from the antistatic wrist strap into the ESD grounding receptacle at the upper right corner of the 6C105.

4. Remove the module from the plastic bag. (Save the bag in the event the module must be reshipped.) Observe all precautions to prevent damage from Electrostatic Discharge (ESD).

5. Examine the module for damage. If any damage is apparent, DO NOT install the module. Immediately contact the Cabletron Systems Global Call Center.

CAUTION

To prevent damaging the backplane connectors in the following step, ensure that the module slides in straight and properly engages the backplane connectors.

NOTE

In the following step, ensure that the top plastic locking tab lines up with the desired slot number located on the front panel of the chassis. Refer to Figure 3-1.

6. Locate the slot guides that line up with the number of the slot in which the module is to be installed. Install the module in the chassis by aligning the module circuit card between the upper and lower metal rail guides of the desired slot, sliding it into the chassis, and locking down the top and bottom plastic locking tabs, as shown in Figure 3-1. Ensure that the module slides in straight and properly engages the backplane connectors.

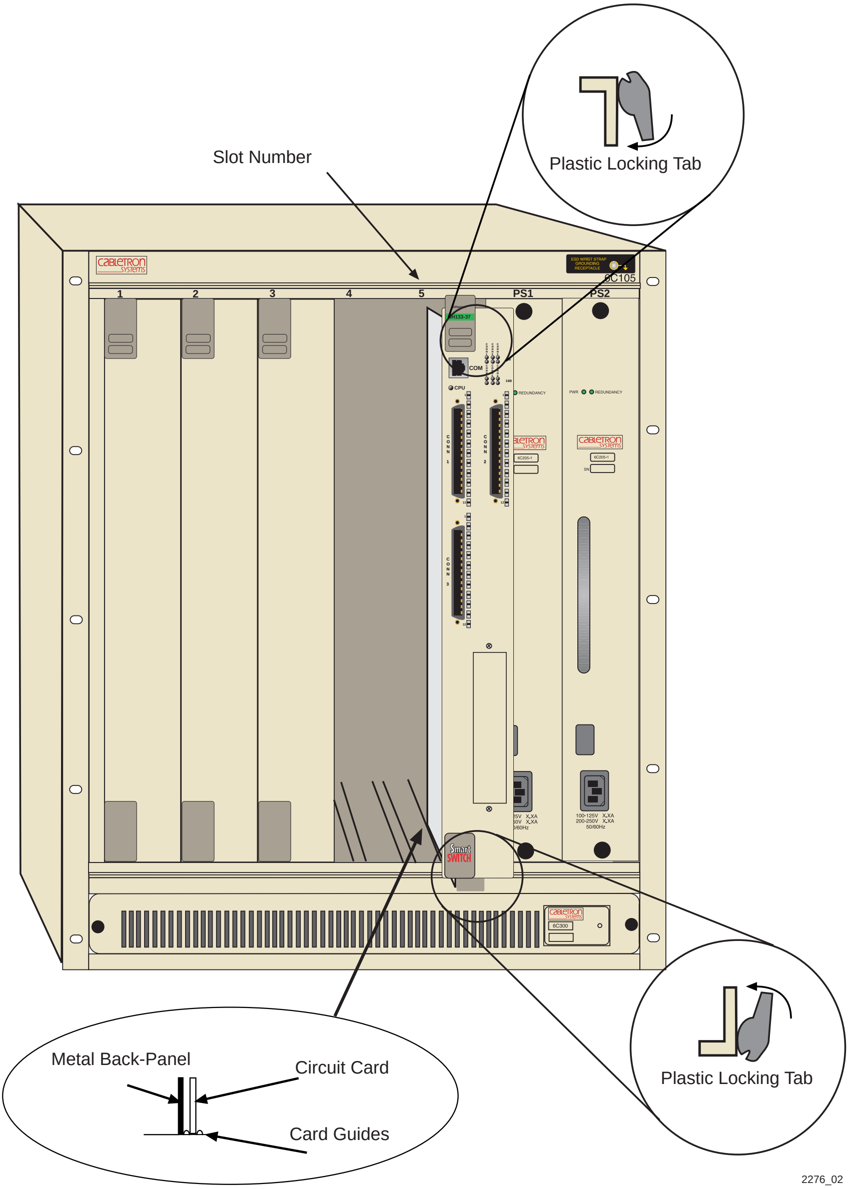


Figure 3-1 Installing an Interface Module

3.5 CONNECTING TO THE NETWORK

This section provides the procedures for connecting UTP and fiber optic segments to the modules.

NOTE

If the device is being installed in a network using SmartTrunking, there are rules concerning the cable connections and port configurations that must be followed for SmartTrunking to operate properly. Before connecting the cables, refer to the Cabletron Systems *SmartTrunk User's Guide* for the configuration information.

The four Ethernet segments and the four Fast Ethernet segments on the 6H123-50 and the three Ethernet segments and the three Fast Ethernet segments on the 6H133-37 can be accessed via RJ21 connectors (CONN 1 through 4 and CONN 1 through 3) for UTP connections. If a port is to operate at 100 Mbps, each pair in a cable must be Category 5 compliant with an impedance of 85 to 111 ohms.

Slots 5 and 6 of the 6H123-50 support FE-100TX, FE-100FX, or FE-100F3 Fast Ethernet Interface Modules. The FE-100TX has an RJ45 connector for a Twisted Pair cable connection. The FE-100FX has an SC style connector for a multimode fiber optic cable connection. The FE-100F3 has an SC style connector for a single mode fiber optic cable connection.

Refer to Section 3.5.1 to make UTP connections to interfaces CONN 1 through 4 and CONN 1 through 3 of the 6H123-50 and 6H133-37.

Refer to Section 3.5.2 to make a Twisted Pair connection to an FE-100TX.

Refer to Section 3.5.3 to make a fiber optic connection to an FE-100FX or FE-100F3.

Refer to the associated High Speed Interface Module user's guide to make connections to an optional High Speed Interface Module installed in the HSIM slot of a 6H133-37.

3.5.1 Connecting UTP Cables

When facing the front panel of the 6H123-50 and 6H133-37, the RJ21 connectors represent Ethernet/Fast Ethernet segments 1 through 8 and segments 1 through 6, respectively.

To connect a UTP segment to the 6H123-50 and 6H133-37, proceed as follows:

1. Ensure that the device connected to the other end of the segment is powered ON.
2. If using an RJ21 straight connector, plug it into the appropriate RJ21 port as shown in Figure 3-2.

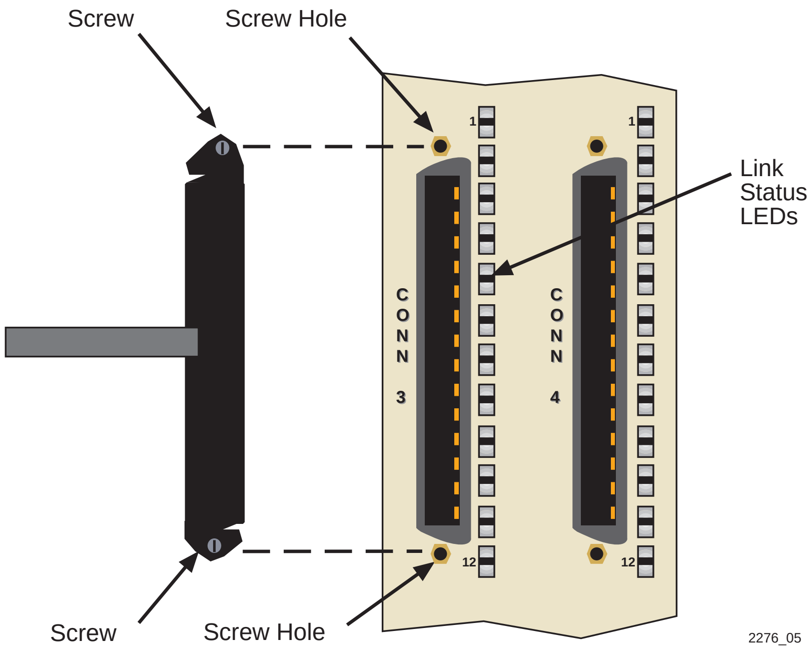


Figure 3-2 Connecting a Twisted Pair Segment

3. Tighten the two screws on the RJ21 connector, as applicable, to secure it to the module.

NOTE

The cable pinouts for a 25-pair cable (RJ21) can be found in the Cabletron Systems *Cabling Guide*. Refer to Section 1.7 for details on how to obtain this document.

4. Verify that a link exists by checking that the port **Link** LEDs are on (flashing amber, blinking green, or solid green). If any of the **Link** LEDs are off, perform the following steps until they are on:

   a. Verify that the device at the other end of the twisted pair segment is ON and connected to the segment.

   b. Verify that the RJ21 connectors on the twisted pair segment have the proper pinouts and check the cable for continuity.

   c. Check that the twisted pair connection meets the dB loss and cable specifications outlined in Chapter 2.

If a link is not established, contact the Cabletron Systems Global Call Center. Refer to Section 1.6 for details.

5. Repeat steps 1 through 5, above, until all RJ21 connections are made.

3.5.2 Connecting a Twisted Pair Segment to the FE-100TX

NOTE

To ensure proper operation, use only Category 5 Unshielded Twisted Pair (UTP) cabling that has an impedance between 85 and 111 ohms.

An FE-100TX installed in slot 5 and/or 6 of the 6H123-50 has an internal crossover switch. When connecting a workstation, use a straight-through cabling and set the Fast Ethernet Interface Module crossover switch shown in Figure 3-3 to the crossed over position marked **X**. When connecting networking devices, such as another bridge, repeater, or router, use a straight-through cable and set the Fast Ethernet Interface Module crossover switch shown in Figure 3-3 to the not crossed over position, marked with =.

If the wires do not cross over, use the switch on the FE-100TX to internally cross over the RJ45 port. Figure 3-3 shows how to properly set the FE-100TX crossover switch.

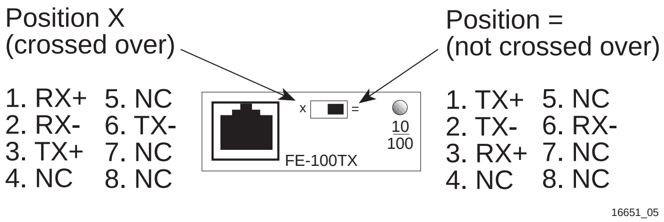


Figure 3-3 FE-100TX Crossover Switch

Connect an FE-100TX to a twisted pair segment as follows:

1. Ensure that the device connected to the other end of the segment is powered ON.
2. Connect the twisted pair segment to the module by inserting the RJ45 connector on the twisted pair segment into the RJ45 port on the module shown in Figure 3-3.
3. Verify that a link exists by checking that the port **RX** LED is on (flashing amber, blinking green, or solid green). If the **RX** LED is off, perform the following steps until it is on:

   a. Verify that the 100BASE-TX device at the other end of the twisted pair segment is powered ON.

   b. Verify that the RJ45 connector on the twisted pair segment has the proper pinouts.

   c. Check the cable for continuity.

   d. Make sure that the twisted pair connection meets dB loss and cable specifications outlined in Section 2.3.

   e. Confirm that the crossover switch is in the correct position.

If a link is not established, contact the Cabletron Systems Global Call Center. Refer to Section 1.6 for details.

3.5.3 Connecting a Fiber Optic Segment to the FE-100FX and FE-100F3

The FE-100FX and FE-100F3 have an SC style network port (see Figure 3-4). Cabletron Systems supplies fiber optic cable that uses SC style connectors that are keyed to ensure proper crossing over of the transmit and receive fibers.

CAUTION

An odd number of crossovers (preferably one) must be maintained between devices so that the transmit port of one device is connected to the receive port of the other device and vice versa.

If the fiber optic cable being used has SC style connectors that do not resemble MIC style connectors, or has SC connectors on one end and a different type on the other, such as ST connectors, ensure that the proper crossing over occurs.

Fiber Optic Network Connection

1. Remove the protective plastic covers from the fiber optic ports on the applicable port on the module and from the ends of the connectors.

CAUTION

The FE-100F3 uses Class 1 lasers. Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, remove power from the network adapter.

CAUTION

Do not touch the ends of the fiber optic strands, and do not let the ends come in contact with dust, dirt, or other contaminants. Contamination of the ends causes problems in data transmissions. If the ends become contaminated, blow the surfaces clean with a canned duster. A fiber port cleaning swab saturated with optical-grade isopropyl alcohol may also be used to clean the fiber optic ends.

2. Insert one end of the SC connector into the FE-100FX or FE-100F3 installed in the 6H123-50. See Figure 3-4.

3. At the other end of the fiber optic cable, attach the SC connector to the other device.

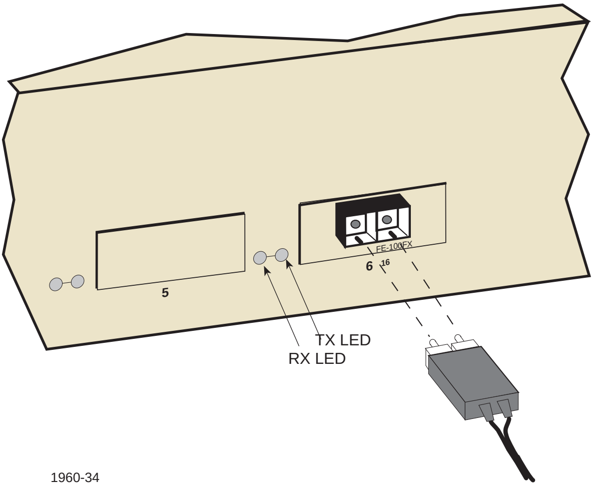


Figure 3-4 Connecting a Fiber Optic Segment

4. Verify that a link exists by checking that the port **RX** LED is on (flashing amber, blinking green, or solid green). If the **RX** LED is off and the **TX** LED is not blinking amber, perform the following steps until it is on:

NOTE

The port **RX** LED flashes green and amber during bootup.

a. Check that the power is turned on for the device at the other end of the link.

b. Verify proper crossing over of fiber strands between the applicable port on the 6H123-50 and the fiber optic device at the other end of the fiber optic link segment.

c. Verify that the fiber connection meets the dB loss specifications outlined in Section 2.4.

If a link has not been established, contact the Cabletron Systems Global Call Center. Refer to Section 1.6 for details.

The 6H123-50 and 6H133-37 are now ready to be set up through Local Management. Refer to Chapter 5 to configure the modules and 6C105 chassis.

CHAPTER 4

TROUBLESHOOTING

This chapter provides information concerning the following:

- Using the LANVIEW diagnostic and status monitoring system (Section 4.1)
- FE-100TX LED (Section 4.2)
- Troubleshooting network and module operational problems (Section 4.3)
- Using the RESET button (Section 4.4)

4.1 USING LANVIEW

The 6H123-50 and 6H133-37 use Cabletron Systems built-in visual diagnostic and status monitoring system called LANVIEW. The LANVIEW LEDs (Figure 4-1) allow quick observation of the network status to aid in diagnosing network problems. Refer to Table 4-1 for a description of the LEDs.

For a functional description of the LANVIEW LED on the optional Fast Ethernet Interface Module (FE-100TX), refer to Section 4.2.

All LEDs for the High Speed Interface Module (HSIM) are located on the HSIM and are described in the associated HSIM user's guide.

NOTE

The terms **flashing**, **blinking**, and **solid** used in the LED definition tables of this chapter indicate the following:

Flashing indicates an irregular LED pulse.

Blinking indicates a steady LED pulse (approximately 50% on and 50% off).

Solid indicates a steady LED light. No pulsing.

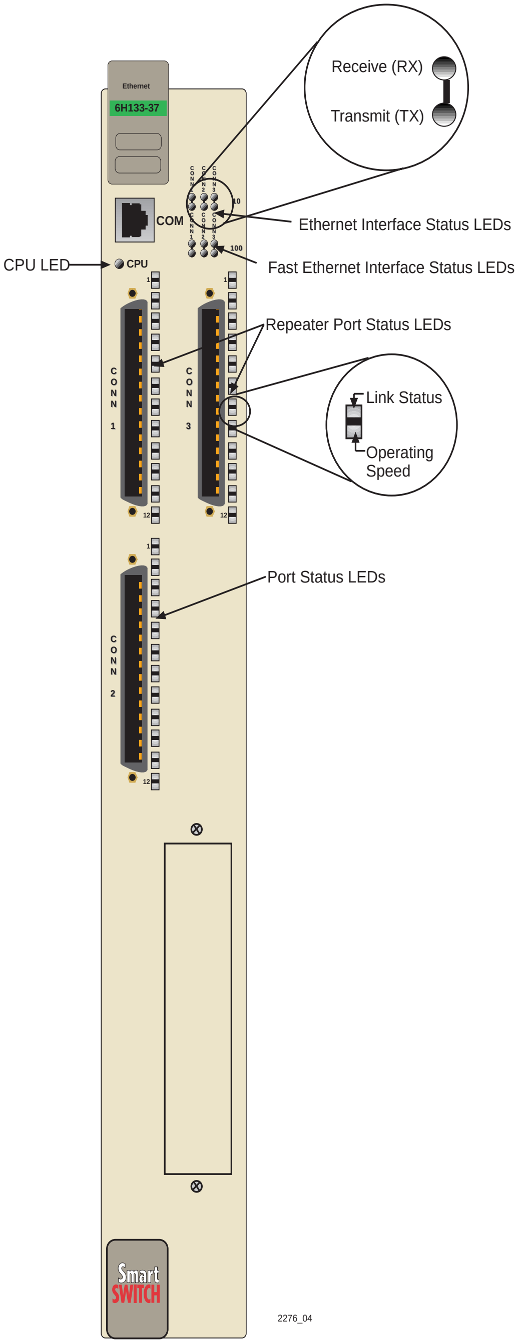


Figure 4-1 LANVIEW LEDs

Table 4-1 LANVIEW LEDs

LED	Color	State	Recommended Action
CPU	Off	Power off.	Power up chassis.
	Red	**Blinking**. Hardware failure has occurred.	Contact the Cabletron Systems Global Call Center.
		Solid. Resetting, normal power up reset.	No action.
	Amber	**Blinking**. Crippled.	Contact the Cabletron Systems Global Call Center.
		Solid. Testing.	No action.
	Green	**Solid**. Functional.	No action.
	Amber and Green	Booting. Blinks amber and green while booting.	No action.
Ethernet Receive Status (RX) of RJ21 Interfaces 10 Mbps Segment	Off	No link. No activity. Port enabled or disabled.	No error.
	Green	**Blinking**. Port disabled, link.	No error.
	Amber	**Flashing**. Port enabled, link, activity.	No error.
	Red	Diagnostic failure.	Contact the Cabletron Systems Global Call Center for assistance.

Table 4-1 LANVIEW LEDs (Continued)

LED	Color	State	Recommended Action
Ethernet Transmit Status (TX) of RJ21 Interfaces 10 Mbps Segment	Off	Port enabled, and no activity. Should flash green every 2 seconds indicating BPDUs being sent if STA is enabled and there is a valid link.	No action.
	Green	**Flashing**. Indicates activity. Rate indicates data rate.	No action.
	Amber	**Blinking**. Port in standby, link. Port may be disabled due to Spanning Tree.	No action.
	Red	**Flashing**. Indicates collision rate.	No action.
		Solid. Diagnostic Failure.	Contact the Cabletron Systems Global Call Center for assistance.
Fast Ethernet Receive Status (RX) of RJ21 Interfaces 100 Mbps Segments and ports 5 and 6 of the 6H123-50	Off	No link. No activity. Port enabled or disabled.	No error.
	Green	**Blinking**. Port disabled, link.	No error.
	Amber	**Flashing**. Port enabled, link, activity.	No error.
	Red	Diagnostic failure.	Contact the Cabletron Systems Global Call Center for assistance.

Table 4-1 LANVIEW LEDs (Continued)

LED	Color	State	Recommended Action
Fast Ethernet Transmit Status (TX) of RJ21 Interfaces 100 Mbps Segments and ports 5 and 6 of the 6H123-50	Off	Port enabled, and no activity. Should flash green every 2 seconds indicating BPDUs being sent if STA is enabled and there is a valid link.	No action.
	Green	**Flashing**. Indicates activity. Rate indicates data rate.	No action.
	Amber	**Blinking**. Port in standby, link. Port may be disabled due to Spanning Tree.	No action.
	Red	**Flashing**. Indicates collision rate.	No action.
		Solid. Diagnostic Failure.	Contact the Cabletron Systems Global Call Center for assistance.
Repeater Port Status Link Status	Off	No Link.	No error.
	Amber	**Flashing**. Receiving data. Flashing indicates data rate.	No error.
	Green	**Blinking**. Port disabled administratively.	No error.
Repeater Port Status Operating Speed Status	Off	Port operating at 10 Mbps, or there is no link to the port.	No error.
	Green	Port operating at 100 Mbps.	No error.

4.2 FE-100TX LED

The optional FE-100TX has one LED labeled 10/100. The 10/100 LED together with the Receive LED allows the user to determine the link status and the operating speed of the Fast Ethernet Interface Module. The 10/100 LED and the Receive (RX) LED are shown in Figure 4-2. Table 4-2 and Table 4-3 provide a functional description of the FE-100TX LED when the RX LED is on or off, respectively.

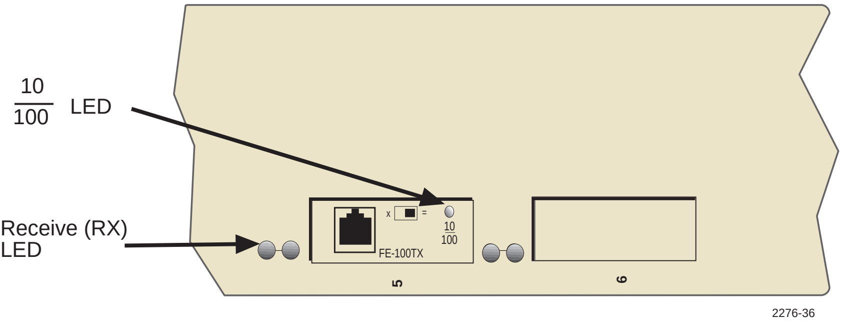


Figure 4-2 FE-100TX LED

NOTE

A link exists if the associated FE-PIM Receive (RX) LED is on.

Table 4-2 FE-100TX LED Indications When the RX LED Is On

LED	Color	Description
10/100	Off	FE-100TX is operating at 10 Mbps.
	Green	FE-100TX is operating at 100 Mbps.

NOTE No link exists if the associated FE-PIM Receive (RX) LED is off.

Table 4-3 FE-100TX LED Indications When the RX LED Is Off

LED	Color	Description
10/100	Off	No link or no cable attached. FE-100TX forced to 10 Mbps operation, or is manually set to “auto-negotiate” mode.
	Green	No link or no cable attached. FE-100TX is forced to 100 Mbps operation.

4.3 TROUBLESHOOTING CHECKLIST

If the 6H123-50 and 6H133-37 are not working properly, refer to Table 4-4 for a checklist of possible problems, causes, and recommended actions to resolve the problem.

Table 4-4 Troubleshooting Checklist

Problem	Possible Cause	Recommended Action
All LEDs are OFF.	Loss of power to the 6C105 chassis.	Check the proper connection of the power cable and its access to a live outlet.
	6H123-50 and 6H133-37 not properly installed.	Check the installation.
No Local Management Password screen.	Autobaud enabled, but baud rate has not yet been sensed.	Press ENTER (RETURN) (may take up to four times).
	Terminal setup is not correct.	Refer to Chapter 5 for proper setup procedures.
	Improper console cable pinouts.	Refer to Appendix A for proper console port pinouts.

Table 4-4 Troubleshooting Checklist (Continued)

Problem	Possible Cause	Recommended Action
Cannot contact the 6H123-50 or 6H133-37 from in-band management.	Improper Community Names Table.	Refer to Section 5.16 for Community Names Table setup.
	6H123-50 or 6H133-37 does not have an IP address.	Refer to Section 5.15.1 for IP address assignment procedure.
	Port is disabled.	Enable port.
	No link to device.	Check link to device.
Port(s) goes into standby for no apparent reason.	6H133-37 or 6H123-50 detects a looped condition.	1. Review network design and delete unnecessary loops. 2. Call the Cabletron Systems Global Call Center if problem continues.
User parameters (IP address, Device and Module name, etc.) are lost when the 6E133-49 or 6E123-50 is powered down.	Mode switch (7), NVRAM Reset, was changed sometime before cycling power causing the user-entered parameters to reset to factory default settings.	1. Reenter the lost parameters as necessary. 2. Call the Cabletron Systems Global Call Center if problem continues.

4.4 USING THE RESET BUTTON

The RESET button, located near the upper plastic locking tab of the module, (refer to Figure 4-3) resets the 6H123-50 and 6H133-37 processor.

CAUTION

Pressing the RESET button resets the device and all current switching being performed by the device is halted. A network downtime of up to two minutes results from this action.

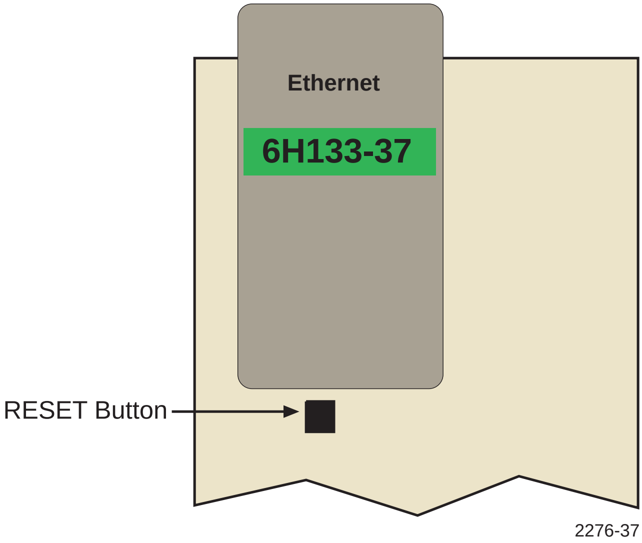


Figure 4-3 RESET Button

To reset the 6H123-50 and 6H133-37 processor, press and release the RESET button. The 6H123-50 and 6H133-37 go through a reset process of approximately 20 seconds. Additional downtime occurs as the module reenters the network.

CHAPTER 5
LOCAL MANAGEMENT

This chapter explains setting up a management terminal to access 6H123-50 and 6H133-37 Local Management. It also explains using the Local Management screens and commands.

NOTE

The Local Management screens shown in this chapter are for the 6H123-50. The 6H133-37 shares most of the following Local Management screens. All Local Management functions specific to any one interface module are preceded by a Note to alert the reader.

5.1 OVERVIEW

Local Management for the 6H123-50 and 6H133-37 consists of a series of management screens that enable the management of the module, the attached segments and the 6C105 chassis. The management screens enable the user to do the following tasks:

- Manage any interface module in the chassis via a connection to a single interface module.
- Assign IP addresses and subnet masks to the 6H123-50, 6H133-37 and the 6C105 chassis.
- Control access to the 6H123-50, 6H133-37 and the 6C105 chassis by establishing community names.
- Download a new image of operating software.
- Designate which Network Management Workstations receive SNMP traps from the 6H123-50, 6H133-37 and the 6C105 chassis.
- Monitor the environmental status of the 6C105 chassis.
- View bridge and port statistics.
- Enable port Trunking to perform load sharing.
- Configure the Fast Ethernet Interface Modules for the 6H123-50 and the HSIM for the 6H133-37.

There are three ways to access Local Management:

- Locally using a VT type terminal connected to the COM port of the 6H123-50 and 6H133-37.
- Remotely using a VT type terminal connected through a modem.
- In-band through a Telnet connection.

5.2 LOCAL MANAGEMENT KEYBOARD CONVENTIONS

Table 5-1 explains the keyboard conventions and the key functions that are used in this manual. All key names appear as capital letters in this manual.

Table 5-1 Keyboard Conventions

Key	Function
ENTER Key RETURN Key	These are selection keys that perform the same Local Management function. For example, “Press ENTER” means that you can press either ENTER or RETURN, unless this manual specifically instructs you otherwise.
ESCAPE (ESC) Key	This key allows an escape from a Local Management screen without saving changes. For example, “Press ESC twice” means the ESC key must be pressed quickly two times.
SPACE bar BACKSPACE Key	These keys cycle through selections in some Local Management fields. Use the SPACE bar to cycle forward through selections and use BACKSPACE to cycle backward through selections.
Arrow Keys	These are navigation keys. Use the UP-ARROW, DOWN-ARROW, LEFT-ARROW, and RIGHT-ARROW keys to move the screen cursor. For example, “Use the arrow keys” means to press whichever arrow key moves the cursor to the desired field on the Local Management screen.
[–] Key	This key decreases values from a Local Management increment field. For example, “Press [–]” means to press the minus sign key.
DEL Key	The DEL (Delete) key removes characters from a Local Management field. For example, “Press DEL” means to press the Delete key.

5.3 MANAGEMENT TERMINAL SETUP

Use one of the following systems to access Local Management:

- An IBM or compatible PC running a VT series emulation software package
- A Digital Equipment Corporation VT100 type terminal
- A VT type terminal running emulation programs for the Digital Equipment Corporation VT100 series
- A remote VT100 type terminal via a modem connection
- In-band via a Telnet connection

5.3.1 Console Cable Connection

Use the Console Cable Kit provided with the 6C105 chassis to attach the management terminal to the COM port as shown in Figure 5-1.

Connect an IBM PC or compatible device, running the VT terminal emulation, to the 6H123-50 and 6H133-37 as follows:

1. Connect the RJ45 connector at one end of the cable (supplied in the kit) to the COM port on the 6H123-50 and 6H133-37.
2. Plug the RJ45 connector on the other end of the cable into the RJ45-to-DB9 adapter (supplied in the kit).
3. Connect the RJ45-to-DB9 adapter to the PC communications port.

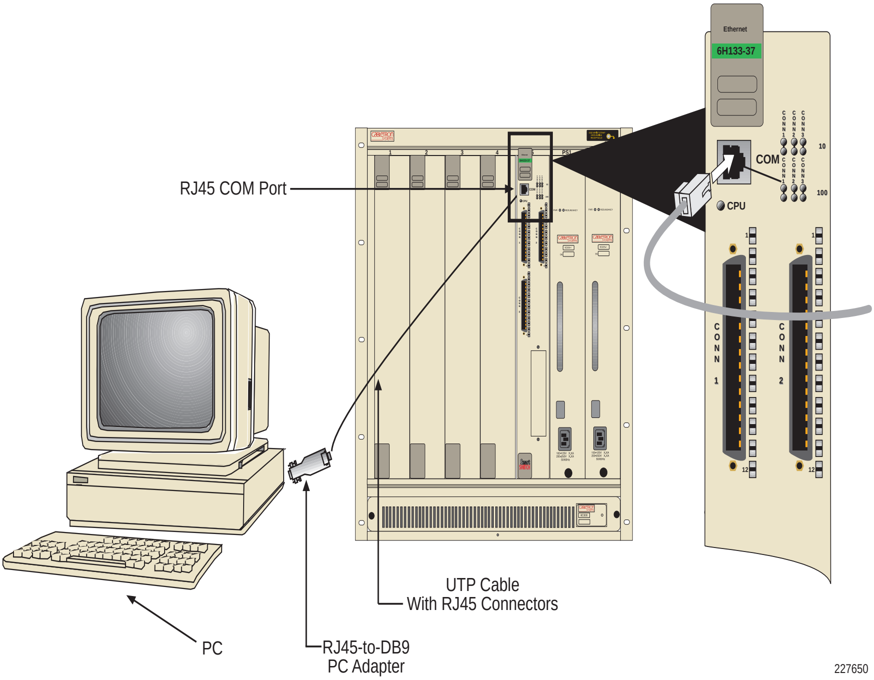


Figure 5-1 Management Terminal Connection

5.3.2 Management Terminal Setup Parameters

Table 5-2 lists the setup parameters for the local management terminal.

Table 5-2 VT Terminal Setup

Display Setup Menu	
Columns ->	80 Columns
Controls ->	Interpret Controls
Auto Wrap ->	No Auto Wrap
Scroll ->	Jump Scroll
Text Cursor ->	Cursor
Cursor Style ->	Underline Cursor Style
General Setup Menu	
Mode ->	VT100, 7 Bit Controls
ID number ->	VT100ID
Cursor Keys ->	Normal Cursor Keys
Power Supply ->	UPSS DEC Supplemental
Communications Setup Menu	
Transmit ->	2400, 4800, 9600, 19200
Receive ->	Receive=Transmit
XOFF ->	XOFF at 64
Bits ->	8 bits
Parity ->	No Parity
Stop Bit ->	1 Stop Bit
Local Echo ->	No Local Echo
Port ->	DEC-423, Data Leads Only
Transmit ->	Limited Transmit
Auto Answerback ->	No Auto Answerback
Keyboard Setup Menu	
Keys ->	Typewriter Keys
Auto Repeat ->	any option
Keyclick ->	any option
Margin Bell ->	Margin Bell
Warning Bell ->	Warning Bell

5.3.3 Telnet Connections

Once the module or chassis has a valid IP address, the user can establish a Telnet session with Local Management from any TCP/IP based node on the network. Telnet connections to the 6H123-50 and 6H133-37 require the community name passwords assigned at the SNMP Community Names screen of either the 6C105 chassis or the module. For additional information about community names, refer to Section 5.8, **SNMP Community Names Screen**. Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

5.3.4 Monitoring an Uninterruptible Power Supply

If the 6C105 chassis is connected to an American Power Conversion (APC) Uninterruptible Power Supply (UPS) for protection from a loss of power, a connection from the COM port of a module to the UPS can be made to monitor the status of the UPS. To use the COM port for this purpose, it must be reconfigured to support the UPS application. This procedure is performed from the General Configuration screen of the interface module. Section 5.15.11, **Configuring the COM Port**, provides detailed instructions on configuring the COM port for UPS applications. Refer to the UPS documentation for details on how to access the status information.

Use the Console Cable Kit provided with the 6C105 chassis to attach the UPS to the module COM port as shown in Figure 5-2.

Connect the UPS device to the COM port of the 6H123-50 and 6H133-37 as follows:

1. Connect the RJ45 connector at one end of the cable to the COM port on the 6H123-50 and 6H133-37.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 male (UPS) adapter, Cabletron Systems Part No. 9372066.
3. Connect the RJ45-to-DB9 male (UPS) adapter to the female DB9 port on the rear of the UPS device (see the particular UPS device’s user instructions for more specific information about the monitoring connection).

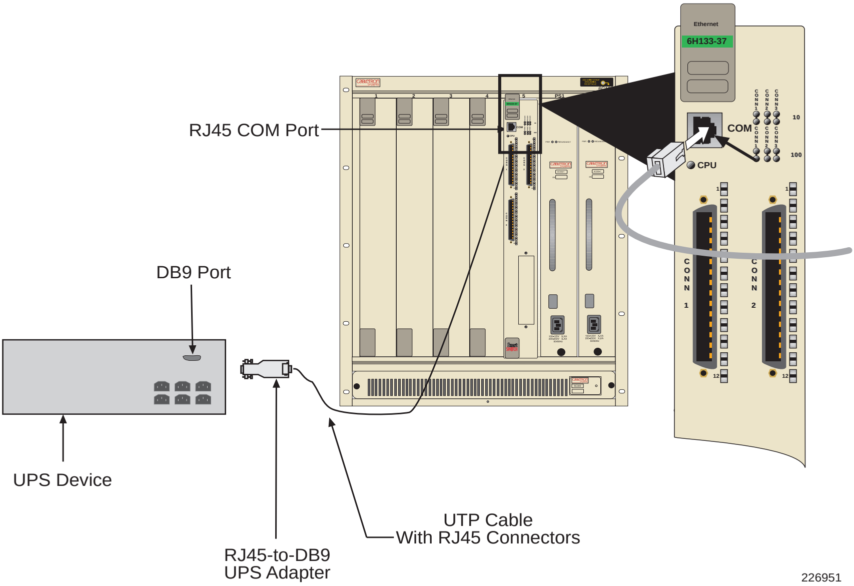
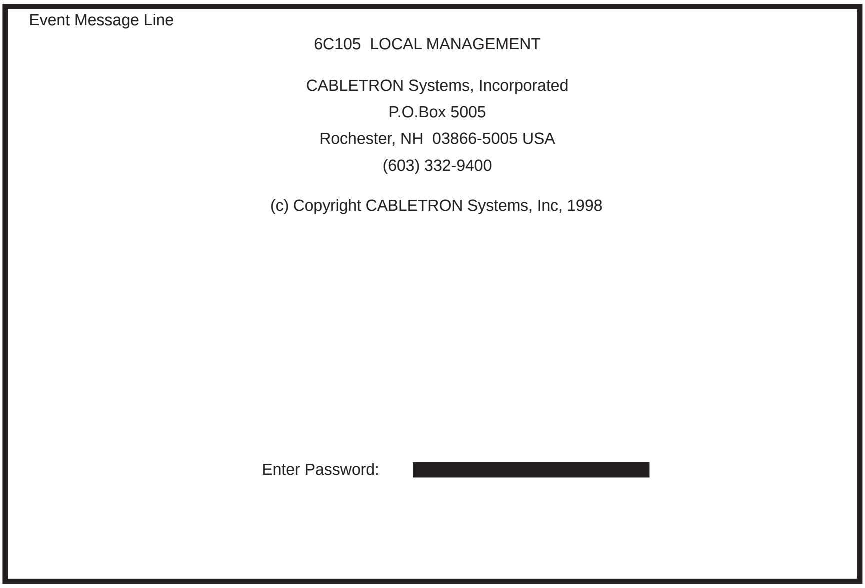


Figure 5-2 Uninterruptible Power Supply (UPS)

5.4 ACCESSING LOCAL MANAGEMENT

Access to Local Management is controlled through the Password screen, Figure 5-3. Whenever a connection is made to the 6H123-50 and 6H133-37 the Password screen displays. Before continuing, the user must enter a password which is compared to the previously stored passwords. The level of access allowed the user depends on the password. To set or change passwords refer to Section 5.8. The following steps describe the procedure to access Local Management.

1. Turn on the terminal. Press ENTER (up to four times) until the 6C105 Local Management Password screen, Figure 5-3, displays.



```
Event Message Line
                         6C105  LOCAL MANAGEMENT

                  CABLETRON Systems, Incorporated
                           P.O.Box 5005
                 Rochester, NH  03866-5005 USA
                          (603) 332-9400

             (c) Copyright CABLETRON Systems, Inc, 1998




             Enter Password:     ███████████████
```

Figure 5-3 Local Management Password Screen

2. Enter the password and press ENTER. The default Super-User access password is “*public*” or press ENTER.

NOTES

The user’s password is one of the community names specified in the SNMP Community Names screen. Access to certain Local Management capabilities depends on the degree of access accorded that community name. Refer to Section 5.8.

If an invalid password is entered, the terminal beeps and the cursor returns to the beginning of the password entry field.

Entering a valid password causes the associated access level to display at the bottom of the screen and the Main Menu screen to appear.

If no activity occurs for several minutes, the Password screen reappears and the session ends.

5.4.1 Navigating Local Management Screens

The 6H123-50 and 6H133-37 Local Management application consists of a series of menu screens. Navigate through Local Management by selecting items from the menu screens.

The 6H123-50 and 6H133-37 support three modes of switch operation. The switching modes are as follows:

- 802.1D Switching (traditional switching)
- 802.1Q Switching (port based switching)
- SecureFast VLAN (Cabletron Systems SecureFast switching)

Depending on the Operational Mode set for the device, the hierarchy of the Local Management screens differs as shown in Figure 5-4, Figure 5-5 and Figure 5-6. Refer to the appropriate figure that relates to the Operational Mode set for the device to see the applicable Local Management screen hierarchy.

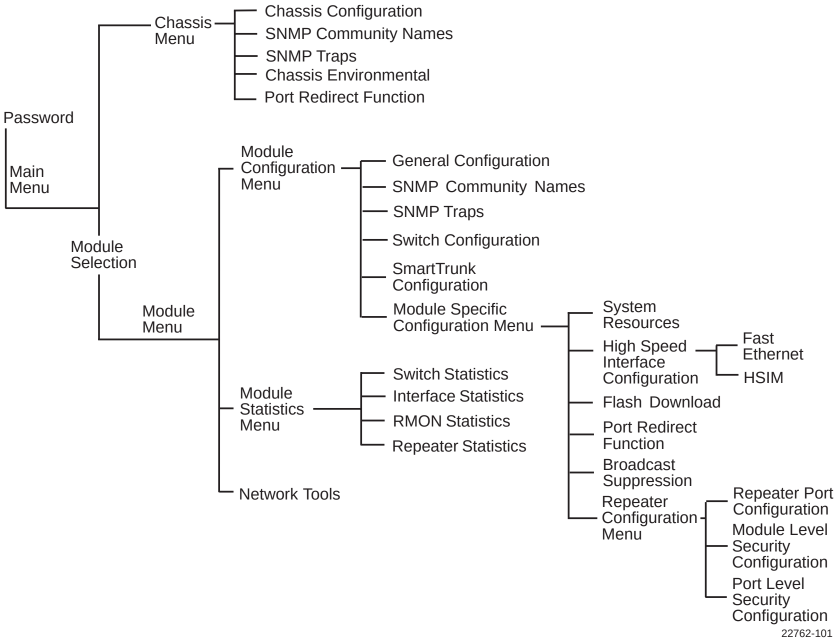


Figure 5-4 Hierarchy of 802.1D Switching Local Management Screens

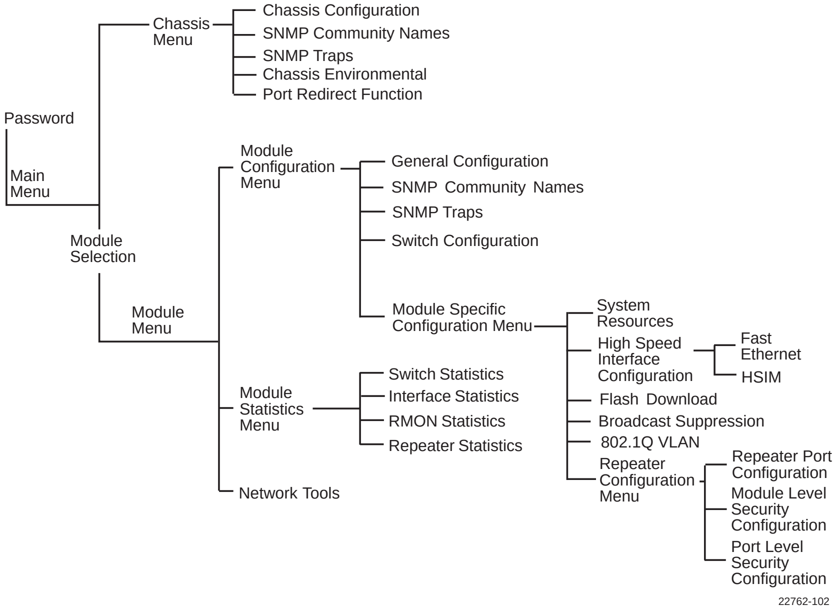


Figure 5-5 Hierarchy of 802.1Q VLAN Local Management Screens

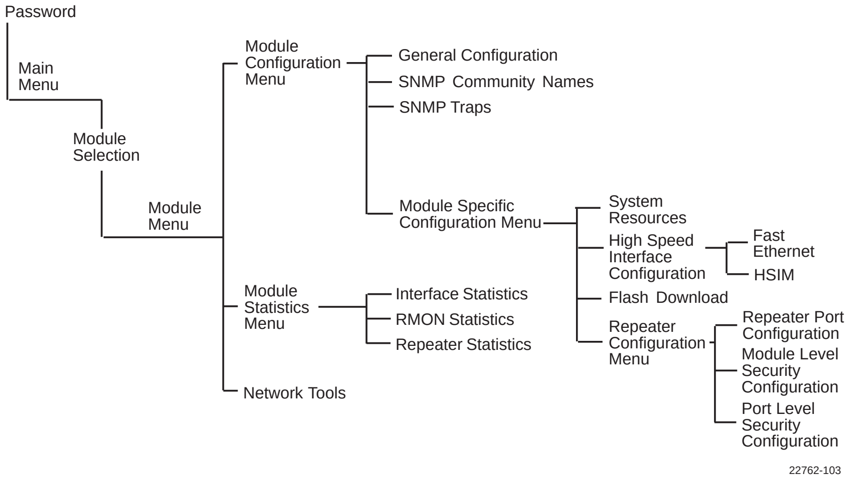


Figure 5-6 Hierarchy of SecureFast Local Management Screens

5.4.2 Selecting Local Management Menu Screen Items

Select items on a menu screen by performing the following steps:

1. Use the arrow keys to highlight a menu item.
2. Press ENTER. The selected menu item displays on the screen.

5.4.3 Exiting Local Management Screens

There are two ways to exit Local Management (LM).

Using the EXIT Command

To exit an LM screen using the **EXIT** command, proceed as follows:

1. Use the arrow keys to highlight the **EXIT** command at the bottom of the Local Management Screen.
2. Press ENTER. The Password screen displays and the session ends.

Using the RETURN Command

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press ENTER. The previous screen in the Local Management hierarchy displays.

NOTE

The user can also exit Local Management screens by pressing ESC twice. This exit method does not warn about unsaved changes and all unsaved changes are lost.

3. Exit from 6H123-50 and 6H133-37 Local Management by repeating steps 1 and 2 until the Main Menu screen displays.
4. Use the arrow keys to highlight the **RETURN** command at the bottom of the Main Menu screen.
5. Press ENTER. The Password screen displays and the session ends.

5.5 MAIN MENU SCREEN

The Main Menu screen is the access point for all Local Management screens for the module and the 6C105 chassis. Figure 5-7 shows the Main Menu screen.

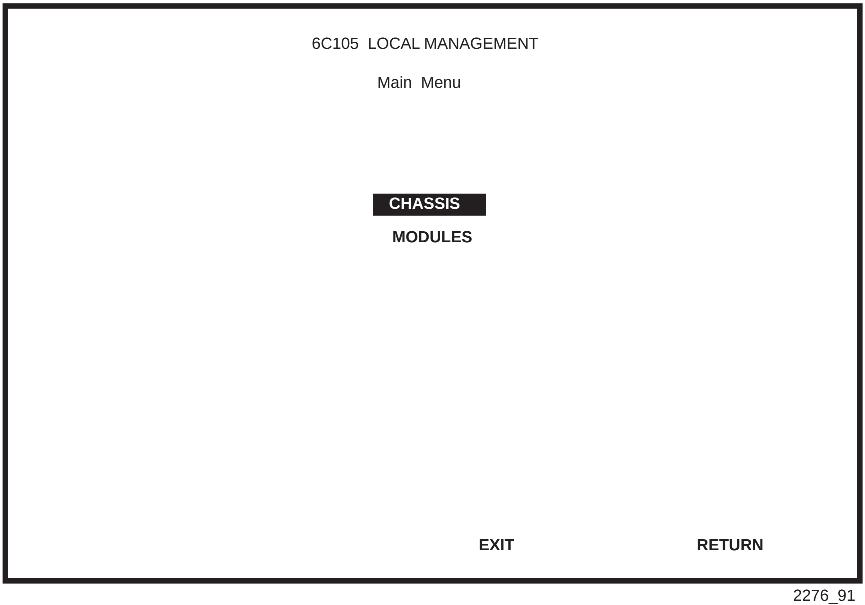


Figure 5-7 Main Menu Screen

The following defines each Main Menu screen menu item as shown in Figure 5-7:

CHASSIS

The Chassis menu item provides access to the Chassis Menu screen, shown in Figure 5-8, that is used to configure the 6C105 chassis and access current chassis power supply and environmental status. For details about the Chassis Configuration screen refer to Section 5.6.

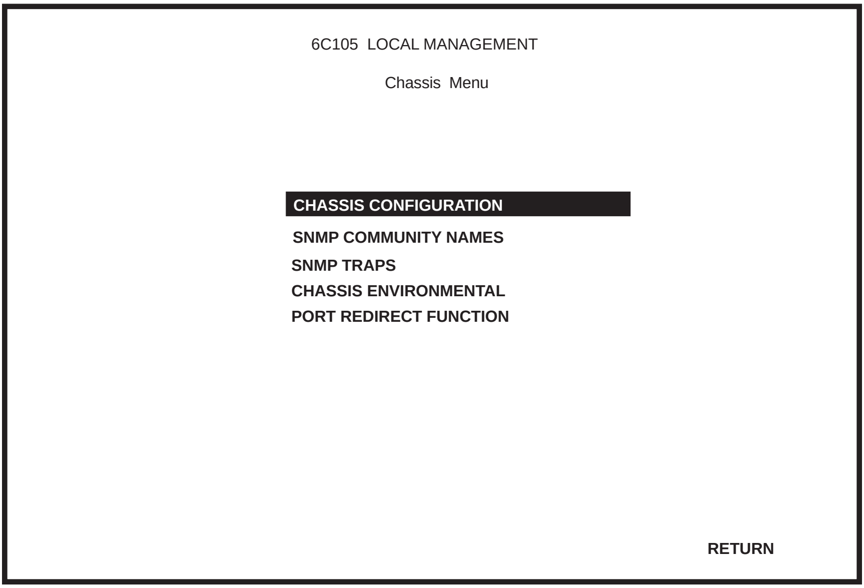
MODULES

The Modules menu item provides access to the Module Selection screen that is used to select individual modules in the chassis for management purposes. For details about the Module Selection screen, refer to Section 5.12.

5.6 CHASSIS MENU SCREEN

The Chassis Menu screen, Figure 5-8, provides access to Local Management screens that enable you to configure and monitor operating parameters, modify SNMP community names, set SNMP traps, monitor the 6C105 environmental status, and perform port redirect functions.

Access the Chassis Configuration screen by using the arrow keys to highlight the CHASSIS menu item and pressing ENTER. The Chassis Configuration screen displays. Proceed to Section 5.6.



22761 99

Figure 5-8 Chassis Menu Screen

The following briefly defines each screen accessible from the Chassis Menu screen.

CHASSIS CONFIGURATION

The Chassis Configuration screen enables the user to configure operating parameters for the 6C105 chassis. For details, refer to Section 5.7.

SNMP COMMUNITY NAMES

The SNMP Community Names screen enables the user to enter new, change, or review the community names used as access passwords for device management operation. Access is limited based on the password level of the user. For details, refer to Section 5.8.

SNMP TRAPS

The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names. For details, refer to Section 5.9.

CHASSIS ENVIRONMENTAL

The Chassis Environmental Information screen provides access to chassis power supply status, power supply redundancy status and chassis fan tray status. For details, refer to Section 5.10.

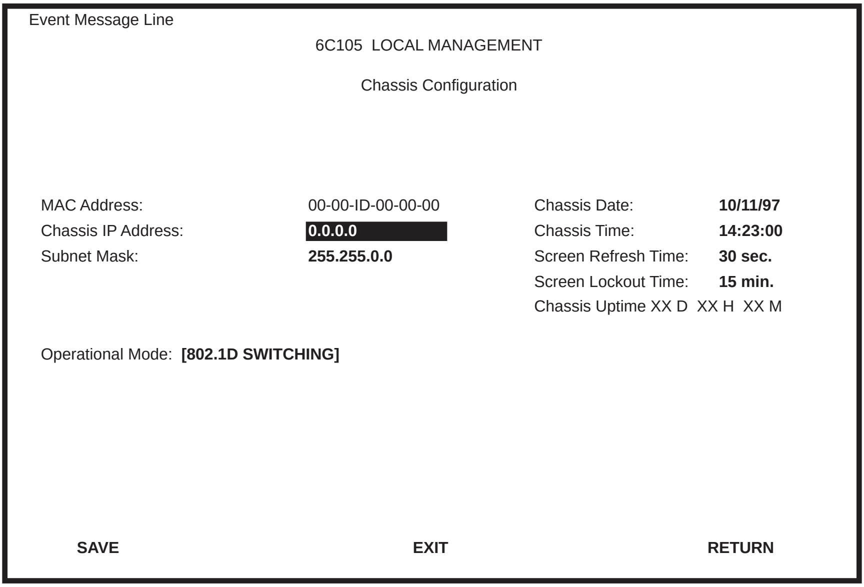
PORT REDIRECT FUNCTION

The Port Redirect Function screen enables the user to redirect traffic from one or multiple modules and ports in the chassis to a specific destination module or port. For details, refer to Section 5.11.

5.7 CHASSIS CONFIGURATION SCREEN

The Chassis Configuration screen, Figure 5-9, enables the user to set the chassis date and time, IP address and Subnet Mask, the operational mode of all modules installed in the chassis, and to view the chassis uptime.

Access the Chassis Configuration screen from the Chassis Menu screen by using the arrow keys to highlight the **CHASSIS CONFIGURATION** menu item and pressing ENTER. The Chassis Configuration screen, Figure 5-9, displays.



```
Event Message Line
                        6C105  LOCAL MANAGEMENT

                          Chassis Configuration


  MAC Address:              00-00-ID-00-00-00     Chassis Date:          10/11/97
  Chassis IP Address:       0.0.0.0               Chassis Time:          14:23:00
  Subnet Mask:              255.255.0.0           Screen Refresh Time:   30 sec.
                                                  Screen Lockout Time:   15 min.
                                                  Chassis Uptime XX D  XX H  XX M

  Operational Mode:  [802.1D SWITCHING]


      SAVE                        EXIT                        RETURN
```

2276_98

Figure 5-9 Chassis Configuration Screen

The following briefly defines each Chassis Configuration screen field:

MAC Address (Read-Only)

Displays the physical address of the chassis.

Chassis IP Address (Modifiable)

This field enables the IP address to be set for the 6C105 chassis. If an IP address is assigned to the 6C105 chassis all the interface modules installed in the chassis can be managed via this IP address, eliminating the need to assign an IP address to each interface module. To set the IP address, refer to Section 5.7.2.

Subnet Mask (Modifiable)

NOTE

When a valid IP address is assigned, the Subnet Mask field automatically enters the default mask that corresponds with class of IP entered in the IP address field. Some firmware revisions do support changing the chassis subnet mask to the default value. Refer to your Release Notes to ensure that the Subnet Mask is a modifiable field.

Displays the subnet mask for the chassis. A subnet mask “masks out” the network bits of the IP address by setting the bits in the mask to 1 when the network treats the corresponding bits in the IP address as part of the network or subnetwork address, or to 0 if the corresponding bit identifies the host. The 6C105 chassis automatically uses the default subnet mask that corresponds to the IP class that was entered in the IP address field.

Chassis Date (Modifiable)

Contains a value that the chassis recognizes as the current date. When the chassis date is modified and saved all interface modules installed in the chassis are set to this date. To set a new chassis date, refer to Section 5.7.3.

Chassis Time (Modifiable)

Contains a value that the chassis recognizes as the current time. When the chassis time is modified and saved, all interface modules installed in the chassis are set to this time. To enter a new time, refer to Section 5.7.4.

Screen Refresh Time (Modifiable)

Contains the rate at which the LM screens are updated. This setting determines how frequently (in seconds) information is updated on the screen. To enter a new update time, refer to Section 5.7.5.

Screen Lockout Time (Modifiable)

Contains the maximum number of minutes that the Local Management application displays a module's screen while awaiting input or action from a user. For example, if the number 5 is entered in this field, the user has up to five minutes to respond to each of the specified module's Local Management screens. In this example, after five minutes of "idleness" (no input or action), the terminal "beeps" five times, the Local Management application terminates the session, and the display returns to the Password screen. To enter a new lockout time, refer to Section 5.7.6.

Chassis Uptime (Read-Only)

Displays the total time the chassis has been operating. The chassis uptime is based on which interface module installed in the chassis has been operating for the longest period of time.

Operational Mode (Selectable)

This field enables the user to set the 6H123-50 and 6H133-37 to operate as an 802.1D switch (Switching option), as a Cabletron Systems SecureFast switch (SFPS VLAN option) or as an 802.1Q switch.

The 12 ports located in each RJ21 interface (CONN 1 through 4 and CONN 1 through 3) are repeater ports, and each Ethernet network, Fast Ethernet network, Fast Ethernet Interface Module, and HSIM port(s) may be bridged to each other.

When the operational mode is set to SFPS VLAN, the 6H123-50 and 6H133-37 act as SecureFast switches. When the Operational Mode is set to 802.1Q switch the 6H123-50 and 6H133-37 are able to increase their switching functionality by creating and maintaining 802.1Q Virtual LANs (VLANs).

For details on how to select the Operation Mode, refer to Section 5.15.9.

5.7.1 Setting the Subnet Mask

If the management workstation that is to receive SNMP traps from the 6C105 is located on a separate subnet, the subnet mask for the 6C105 must be changed from its default.

To change the subnet mask from its default, perform the following steps:

NOTE

When a valid IP address is assigned, the Subnet Mask field automatically enters the default mask that corresponds with class of IP entered in the IP address field. Some firmware revisions do support changing the chassis subnet mask to the default value. Refer to your Release Notes to ensure that the Subnet Mask is a modifiable field.

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the subnet mask into this field using Decimal Dotted Notation (DDN) format.

   For example: 255.255.255.0
3. Press ENTER. If the subnet mask is valid, the cursor returns to the beginning of the Subnet Mask field. If the entry is not valid, the Event Message Line displays “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Subnet Mask field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The changes are saved to memory.

5.7.2 Setting the IP Address

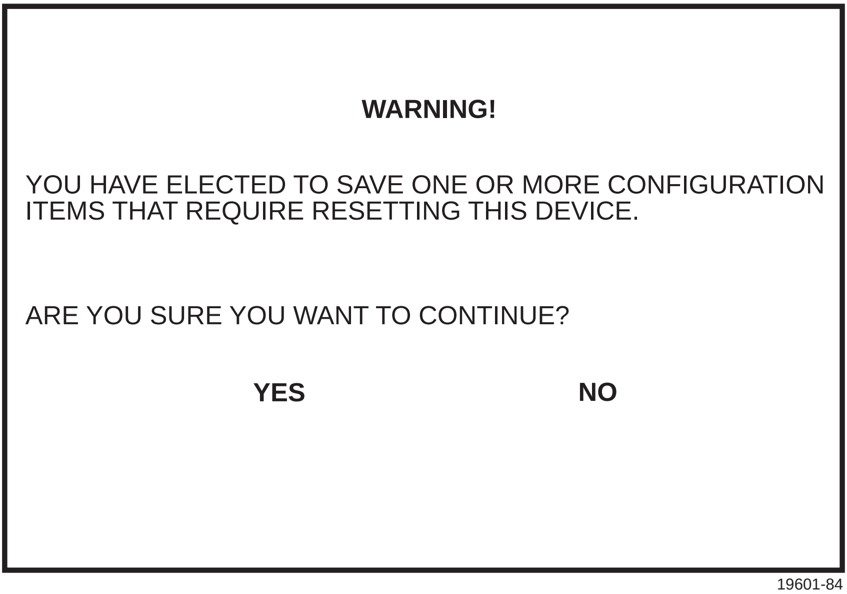
To set the IP address, perform the following steps:

1. Use the arrow keys to highlight the **IP Address** field.
2. Enter the IP address into this field using Decimal Dotted Notation (DDN) format.

   For example: 134.141.79.120

3. Press ENTER. If the IP address is a valid format, the cursor returns to the beginning of the IP address field. If the entry is not valid, the Event Message Line displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the IP address field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-10 displays.



WARNING!

YOU HAVE ELECTED TO SAVE ONE OR MORE CONFIGURATION ITEMS THAT REQUIRE RESETTING THIS DEVICE.

ARE YOU SURE YOU WANT TO CONTINUE?

Figure 5-10 Configuration Warning Screen

5. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.

5.7.3 Setting the Chassis Date

NOTE

The 6C105 is year 2000 compliant, so the Chassis Date may be set beyond the year 1999.

To set the chassis date, perform the following steps:

1. Use the arrow keys to highlight the **Chassis Date** field.
2. Enter the date in this format: MM/DD/YYYY

NOTE

It is not necessary to add separators between month, day, and year numbers. For example, to set the date to 03/17/1997, type “03171997” in the Chassis Date field.

3. Press ENTER to set the system calendar to the date in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value, but it does refresh the Chassis Date field with the previous value.

NOTE

Upon saving the new chassis date, all interface modules installed in the chassis recognize the new value as the current date.

5.7.4 Setting the Chassis Time

To set the chassis clock, perform the following steps:

1. Use the arrow keys to highlight the **Chassis Time** field.
2. Enter the time in this 24-hour format: HH:MM:SS

NOTE

When entering the time in the system time field, separators between hours, minutes, and seconds do not need to be added as long as each entry uses two numeric characters. For example, to set the time to 6:45 A.M., type “064500” in the Chassis Time field.

3. Press ENTER to set the system clock to the time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value and refreshes the Chassis Time field with the previous value.

NOTE

Upon saving the new chassis time, all interface modules installed in the chassis recognize the new value as the current time.

5.7.5 Entering a New Screen Refresh Time

The screen refresh time is set from 3 to 99 seconds with a default of 3 seconds. To set a new screen refresh time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Refresh Time** field.
2. Enter a number from 3 to 99.
3. Press ENTER to set the refresh time to the time entered in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 3 to 99 seconds range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Refresh Time field with the previous value.

5.7.6 Setting the Screen Lockout Time

The screen lockout time can be set from 1 to 30 minutes with a default of 15 minutes. To set a new lockout time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Lockout Time** field.
2. Enter a number from 1 to 30.
3. Press ENTER to set the lockout time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 1 to 30 minutes range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Lockout Time field with the previous value.

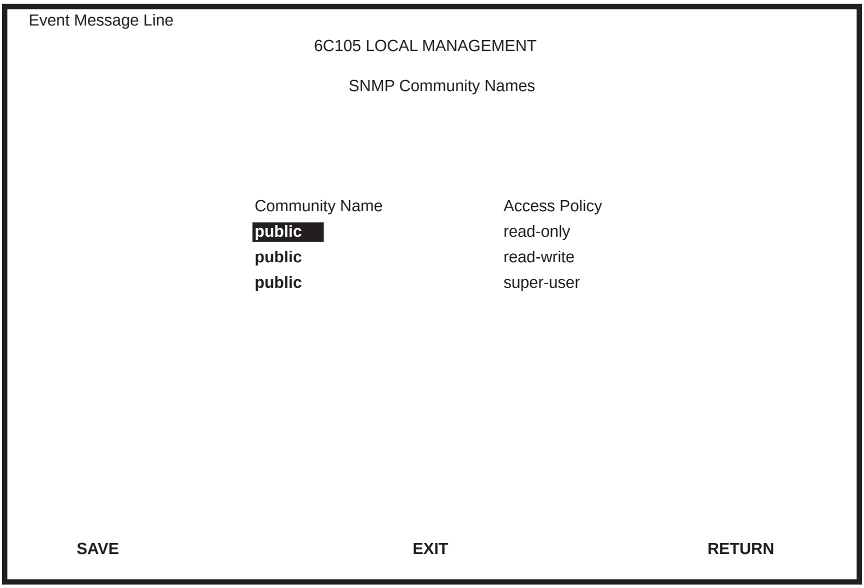
5.8 SNMP COMMUNITY NAMES SCREEN

The SNMP Community Names screen enables the user to set Local Management community names. Community names act as passwords to Local/Remote Management and provide security access to the 6C105. Access to the 6C105 is controlled by enacting any of three different levels of security authorization (read-only, read-write, and super-user).

NOTE

Super-User access gives the user full management privileges, allows existing passwords to be changed, and all modifiable MIB objects for the Cabletron Container MIB and Internet MIB-II to be edited.

Access the SNMP Community Names screen from the Chassis Configuration screen by using the arrow keys to highlight the **SNMP COMMUNITY NAMES** menu item and pressing ENTER. The SNMP Community Names screen, Figure 5-11, displays.



Event Message Line

6C105 LOCAL MANAGEMENT

SNMP Community Names

Community Name	Access Policy
public	read-only
public	read-write
public	super-user

Figure 5-11 SNMP Community Names Screen

The following defines each SNMP Community Names screen field:

Community Name (Modifiable)

Displays the user-defined name through which a user accesses 6C105 management. Any community name assigned here acts as a password to Local/Remote Management.

Access Policy (Read-Only)

Indicates the access accorded each community name. Possible selections are as follows:

read-only — This community name allows read-only access to the 6C105 MIB objects, and excludes access to security-protected fields of read-write or super-user authorization.

read-write — This community name allows read and write access to the 6C105 MIB objects, excluding security protected fields for super-user access only.

super-user — This community name permits read-write access to the 6C105 MIB objects and allows the user to change all modifiable parameters including community names, IP addresses, traps, and SNMP objects.

5.8.1 Establishing Community Names

The password used to access Local Management at the Password Screen must have Super-User access in order to view and edit the SNMP Community Names screen. Using a password with read-only or read-write access does not enable the user to view or edit the SNMP Community Names screen.

NOTE

Any community name assigned in the SNMP Community Names screen is a password to its corresponding level of access to Local Management. The community name assigned Super-User access is the only one that gives the user complete access to Local Management.

NOTE

All passwords assigned in the 6C105 SNMP Community Names screen allow access to both 6C105 Local Management screens, and the Local Management screens of the interface modules that are installed in the chassis. To configure the interface module to not allow access to 6C105 Local Management screens refer to Section 5.16.

To establish community names, proceed as follows:

1. Use the arrow keys to highlight the **Community Name** field adjacent to the selected access level.
2. Enter the password in the field (maximum 31 characters).
3. Press ENTER.
4. Repeat steps 1 through 3 to modify the other community names.
5. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER. The message “SAVED OK” displays. The community names are saved to memory and their access modes implemented.

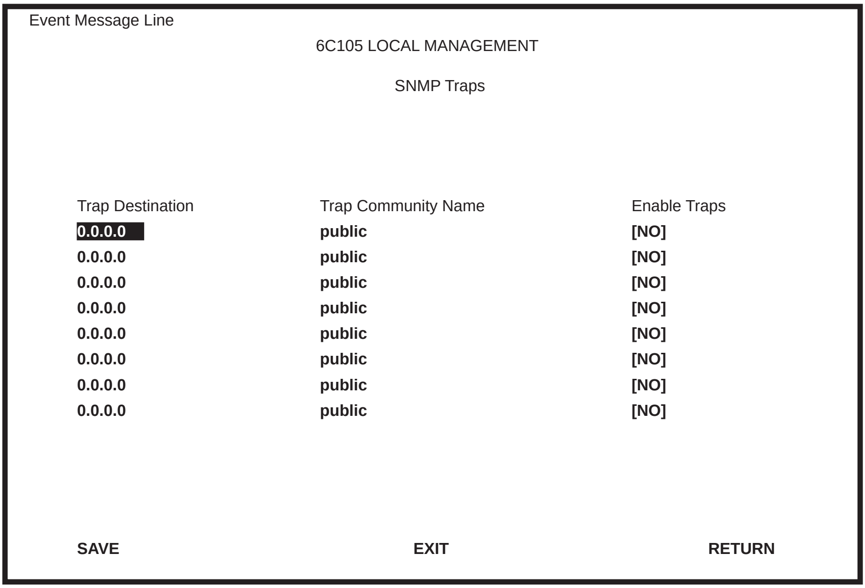
NOTE

Exiting without saving causes a “NOT SAVED?” message to display above the **SAVE** command. Edits are lost if they are not saved before exiting.

5.9 SNMP TRAPS SCREEN

Since the 6C105 is an SNMP compliant device, it can send messages to multiple Network Management Stations to alert users of status changes. This is set up using the SNMP Traps screen. The SNMP Traps screen is shown in Figure 5-12.

Access the SNMP Traps screen from the Chassis Configuration screen by using the arrow keys to highlight the **SNMP TRAPS** menu item and pressing ENTER. The SNMP Traps screen displays.



```
 Event Message Line
                              6C105 LOCAL MANAGEMENT

                                   SNMP Traps



      Trap Destination          Trap Community Name           Enable Traps
      0.0.0.0                   public                        [NO]
      0.0.0.0                   public                        [NO]
      0.0.0.0                   public                        [NO]
      0.0.0.0                   public                        [NO]
      0.0.0.0                   public                        [NO]
      0.0.0.0                   public                        [NO]
      0.0.0.0                   public                        [NO]
      0.0.0.0                   public                        [NO]



      SAVE                              EXIT                        RETURN
```

1960_17

Figure 5-12 SNMP Traps Screen

The following defines each field of the SNMP Traps screen.

Trap Destination (Modifiable)

Indicates the IP address of the workstation to receive trap alarms. Up to eight different destinations can be defined.

Trap Community Name (Modifiable)

Displays the Community Name included in the trap message sent to the Network Management Station with the associated IP address.

Enable Traps (Toggle)
Enables transmission of the traps to the network management station with the associated IP address. This field toggles between YES and NO.

5.9.1 Configuring the Trap Table

To configure the trap table, proceed as follows:

1. Using the arrow keys, highlight the appropriate **Trap Destination** field.
2. Enter the IP address of the workstation that is to receive traps. IP address entries must follow the DDN format.

   For example: 134.141.79.121
3. Press ENTER. If an invalid entry is made “INVALID IP ENTERED” displays in the Event Message Line.
4. Using the arrow keys, highlight the **Trap Community Name** field. Enter the community name.
5. Press ENTER.
6. Using the arrow keys, highlight the **Enable Traps** field. Press the SPACE bar to choose either **YES** (send alarms from the chassis to the workstation), or **NO** (prevent alarms from being sent).
7. Using the arrow keys, highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays on the screen.

NOTE

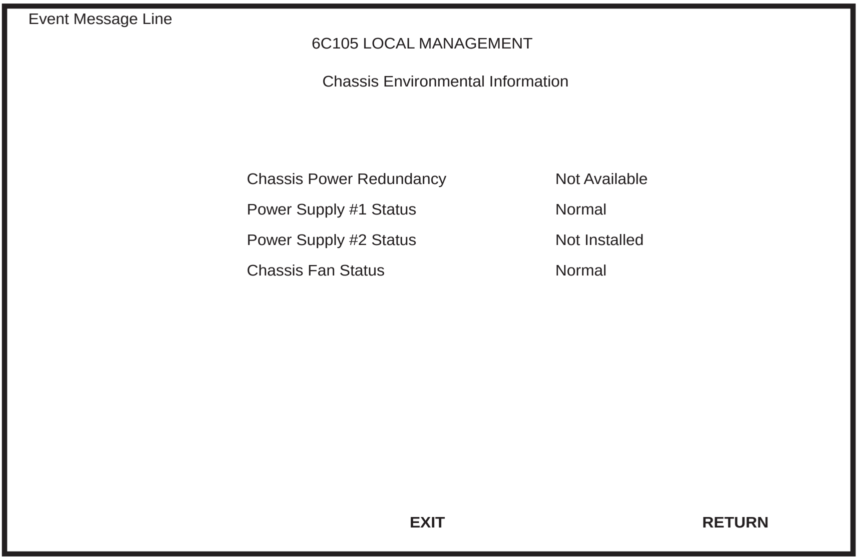
Exiting without saving causes a “NOT SAVED?” message to appear above the **SAVE** command. Edits will be lost if they are not saved before exiting.

The designated workstations now receive traps from the 6C105.

5.10 CHASSIS ENVIRONMENTAL INFORMATION SCREEN

The Chassis Environmental Information screen enables the user to view chassis environmental information.

Access the Chassis Environmental Information screen from the Chassis Menu screen by using the arrow keys to highlight the **CHASSIS ENVIRONMENTAL** menu item and pressing ENTER. The Chassis Environmental Information screen, Figure 5-13, displays.



```
Event Message Line
                    6C105 LOCAL MANAGEMENT

                 Chassis Environmental Information


        Chassis Power Redundancy          Not Available
        Power Supply #1 Status            Normal
        Power Supply #2 Status            Not Installed
        Chassis Fan Status                Normal
```

2276_94

Figure 5-13 Chassis Environmental Information Screen

The following describes each of the Chassis Environmental Information screen fields.

Chassis Power Redundancy (Read-Only)

Displays the current redundancy status of the 6C105 power supplies. This field will read either “Available” or “Not Available”.

Power Supply #*X* Status (Read-Only)

Displays the current status of power supplies 1 and 2 for the 6C105. This field will read either “Normal”, “Fault”, or “Not Installed”.

chassis Fan Status (Read-Only)
Displays the current status of the 6C105 fan tray. This field will read either “Normal”, “Fault”, or “Not Installed”.

5.11 PORT REDIRECT FUNCTION SCREEN

The Port Redirect Function screen, Figure 5-14, enables the user to set each one of the modules in the chassis (1 through 5), and the interfaces (bridge ports) of the corresponding module installed, as a source or destination interface. An interface can be set to have one or more destination interface and chassis module slot numbers.

For example, interface (port) 1 in module (slot) 1 can be set as a source interface with three destinations, interfaces 2, 3, and 4 in module (slot) 3. Traffic from interface 1 in module 1 is then automatically redirected to interfaces 2, 3, and 4 in module 3. Interface 1 in module 1 can also serve as a destination interface for other interfaces and modules. The port redirect function is extremely useful for troubleshooting purposes, as it allows traffic to be sent to a particular interface(s) where, with the use of an analyzer or RMON probe, all current traffic from the source interface(s) can be examined.

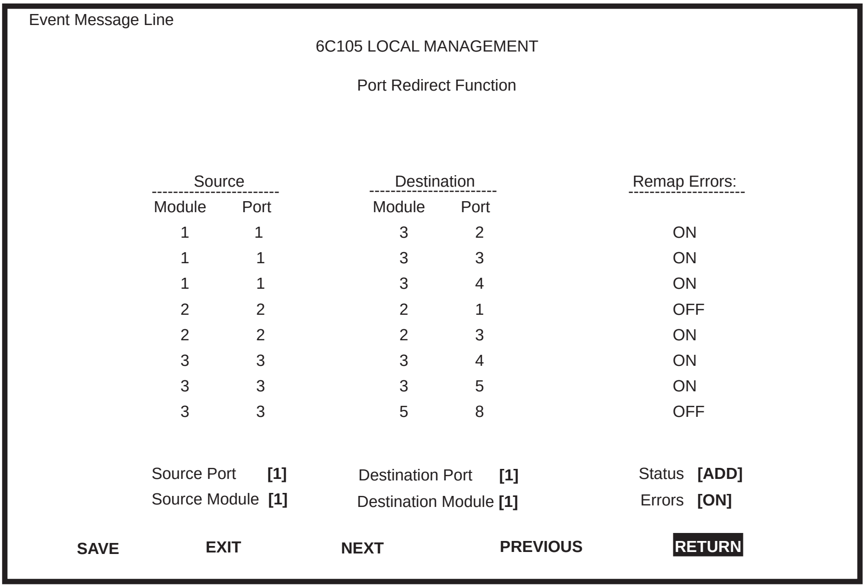
Port Redirect operates at a switch interface level and not at a repeater port level. If traffic is redirected to interfaces that include active repeater ports attached then the redirected traffic is transmitted out all of the repeater ports connected to the interface.

NOTES

The module number corresponds to the slot number in which the module resides in the 6C105 chassis (1 through 5).

Although traffic from the source interface (including, if desired, errored frames) is sent to the destination interface, normal switching is still performed for all frames on the source interface.

Access the Port Redirect Function screen from the Chassis Menu screen by using the arrow keys to highlight the **PORT REDIRECT FUNCTION** menu item and pressing ENTER. The Port Redirect Function screen, Figure 5-14, displays.



```
Event Message Line
                              6C105 LOCAL MANAGEMENT

                                Port Redirect Function



               Source                   Destination                 Remap Errors:
       -------------------------  -------------------------     ----------------------
        Module      Port           Module      Port
          1           1              3           2                    ON
          1           1              3           3                    ON
          1           1              3           4                    ON
          2           2              2           1                    OFF
          2           2              2           3                    ON
          3           3              3           4                    ON
          3           3              3           5                    ON
          3           3              5           8                    OFF


       Source Port       [1]      Destination Port      [1]      Status   [ADD]
       Source Module  [1]         Destination Module [1]         Errors   [ON]

   SAVE          EXIT          NEXT           PREVIOUS          RETURN
```

2276_22

Figure 5-14 Port Redirect Function Screen

The following definitions briefly define each field of the Port Redirect Function screen.

Source Module (Read-Only)

Displays which modules are currently set as source modules.

Source Port (Read-Only)

Displays which ports are currently set as source ports.

Destination Module (Read-Only)

Displays which modules are currently set as destination modules.

Destination Port (Read-Only)

Displays which ports are currently set as destination ports.

Remap Errors (Read-Only)

Displays ON or OFF to indicate whether the corresponding source modules and ports are configured to send errored frames to the destination modules and ports (ON), or to drop all errored frames before forwarding traffic (OFF).

Source Module [*n*] (Selectable)
Used to select a module [*n*] as a source module.

Source Port [*n*] (Selectable)
Used to select a port [*n*] as a source port.

Destination Module [*n*] (Selectable)
Used to select a module [*n*] as a destination module.

Destination Port [*n*] (Selectable)
Used to selected a port [*n*] as a destination port.

Errors (Toggle)
Used to configure the selected source port to either send errored frames to a selected destination port (ON option), or to drop errored frames, and send only valid traffic to the destination port (OFF option). The default option is ON.

Status (Toggle)
Used to add or delete source/destination ports selected in the Source/Destination Ports fields.

5.11.1 Displaying the Source and Destination Entries

There can be more than one Port Redirect Function screen depending on the number of port redirect entries. Each screen displays up to ten port redirect entries. If there is more than one screen of redirect entries, the NEXT and/or PREVIOUS command displays at the bottom of the screen, allowing the user to navigate to the next or previous screen.

For example, with three screens of entries, the NEXT command displays at the bottom of the first screen. In the second screen, the NEXT and PREVIOUS commands display. In the last screen, only the PREVIOUS command displays.

To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER and the next screen of entries displays.

To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries in the previous screen.

5.11.2 Changing Source and Destination Ports

Add or delete source/destination module and port entries as follows:

1. Use the arrow keys to highlight the **Source Module** field.
2. Press the SPACE bar or BACKSPACE one or more times to increment or decrement the module number displayed in the brackets [*n*] until the appropriate module number displays.
3. Use the arrow keys to highlight the **Source Port** field.
4. Press the SPACE bar or BACKSPACE one or more times to increment or decrement the port number displayed in the brackets [*n*] until the appropriate port number displays.
5. Use the arrow keys to highlight the **Destination Module** field.
6. Use the SPACE bar or BACKSPACE to step to the appropriate module number for the destination module.
7. Use the arrow keys to highlight the **Destination Port** field.
8. Use the SPACE bar or BACKSPACE to step to the appropriate port number for the destination port.
9. Use the arrow keys to highlight the **Errors** field.
10. Press the SPACE bar to select **ON** or **OFF**, then press ENTER. **ON** forces the source module and port to forward errored frames to the destination module and port. OFF forces the errored frames to be dropped before forwarding traffic.
11. Use the arrow keys to highlight the **Status** field.
12. Use the SPACE bar to select either the **ADD** or **DEL** (delete) option. Press ENTER. This adds or deletes the port selections made in steps 2 and 4 and also updates the screen Source Port and Destination Port list.

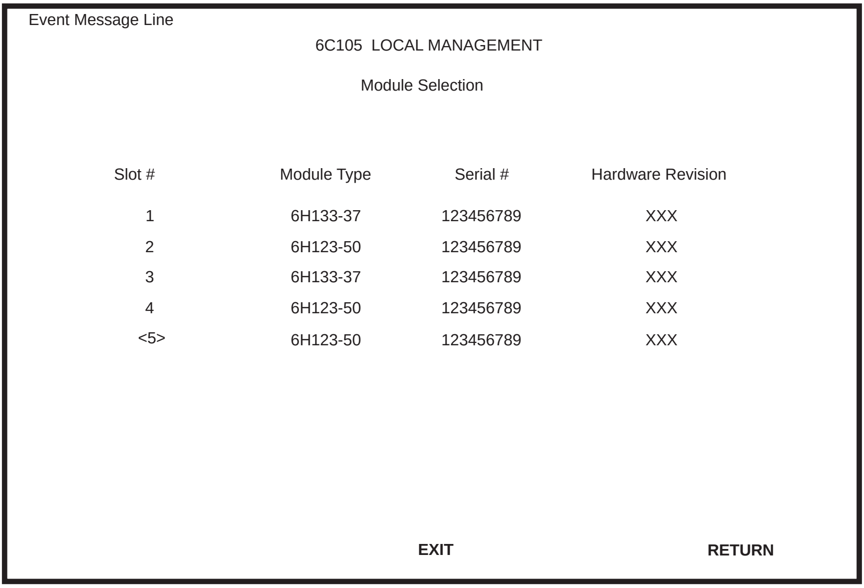
NOTE

If more than one port is to be redirected, repeat steps 1 through 6 for each additional setting, then go to step 7 to save all the new settings at once.

13. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The message “SAVED OK” displays. This saves the new settings and updates the Source Port and Destination Port read-only fields.

5.12 MODULE SELECTION SCREEN

The Module Selection screen is the access point to Local Management for all modules installed in the SmartSwitch 6000 chassis. By selecting a module, the user accesses the Module Menu screen for the selected device. Figure 5-15 shows the Module Selection screen.



```
  Event Message Line
                                6C105  LOCAL MANAGEMENT

                                   Module Selection


        Slot #            Module Type        Serial #        Hardware Revision

          1                 6H133-37         123456789              XXX
          2                 6H123-50         123456789              XXX
          3                 6H133-37         123456789              XXX
          4                 6H123-50         123456789              XXX
         <5>                6H123-50         123456789              XXX




                                       EXIT                              RETURN
```

2276-39

Figure 5-15 Module Selection Screen

The following defines each Module Selection screen field as shown in Figure 5-15.

Slot # (Selectable)
The Slot # field displays the slot in which the module is installed. The module number enclosed in < > characters indicates the module to which the management terminal is connected or the Telnet session has been established.

Module Type (Read-Only)
The Module Type field displays the type of interface module that is installed in each slot.

Serial # (Read-Only)
Indicates the serial number of the module. The serial number of the device is necessary when calling the Cabletron Systems Global Call Center.

Hardware Revision (Read-Only)
Shows the hardware revision of the module.

5.12.1 Selecting a Module

To select an individual module to perform Local Management functions, proceed as follows:

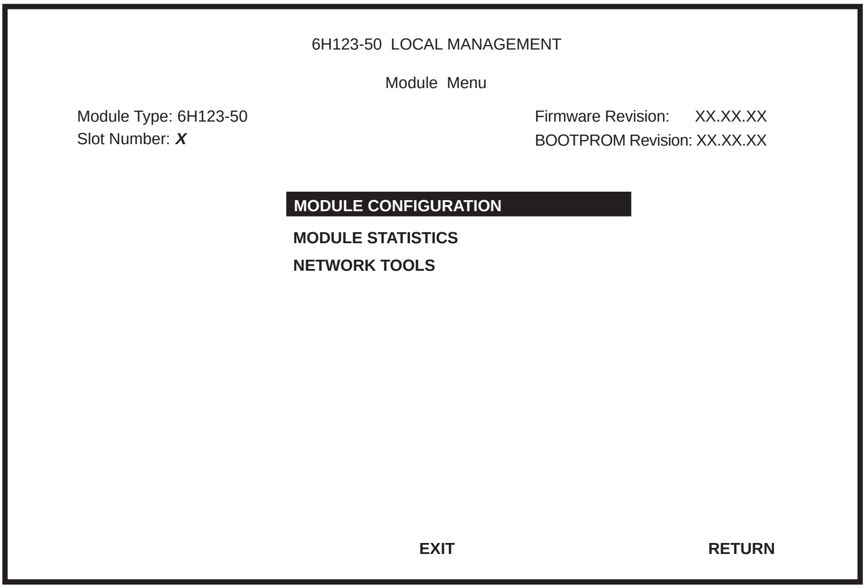
1. Use the arrow keys to highlight the desired module number in the **Slot #** field.
2. Press ENTER, the applicable Module Menu screen displays.

5.13 MODULE MENU SCREEN

NOTE

The Local Management screens shown in this chapter are for the 6H123-50. The 6H133-37 shares most of the following Local Management screens. All Local Management functions specific to any one interface module are preceded by a Note to alert the reader.

The Module Menu screen is the access point for all Local Management screens for the 6H123-50 and 6H133-37. Figure 5-16 shows the 6H123-50 Module Menu screen.



6H123-50 LOCAL MANAGEMENT

Module Menu

Module Type: 6H123-50
Slot Number: ***X***

Firmware Revision: XX.XX.XX
BOOTPROM Revision: XX.XX.XX

2276_13

Figure 5-16 Module Menu Screen

The following defines each Module Menu screen field as shown in Figure 5-16:

MODULE CONFIGURATION

Accesses the Local Management screens that are used to configure the 6H123-50 and 6H133-37 and the Module Specific Configuration Menu screen. The Module Specific Configuration Menu screen provides access to the screens that enable the user to check 6H123-50 and 6H133-37 resources and set operating parameters specific to each port. For details about the Module Configuration Menu screen, refer to Section 5.14. For details about the Module Specific Configuration menu screen, refer to Section 5.19.

MODULE STATISTICS

Accesses the Module Statistics Menu screen, which provides access to screens that enable the user to obtain switch, interface, RMON and repeater information for the 6H123-50 and 6H133-37. For details about these screens, refer to Section 5.30.

NETWORK TOOLS

Accesses the Network Tools, which resides on the 6H123-50 and 6H133-37 and consists of a series of commands that enable the user to access and manage network devices. Section 5.35 explains how to use the Network Tools utility.

5.14 MODULE CONFIGURATION MENU SCREEN

The Module Configuration Menu screen, Figure 5-17, provides access to Local Management screens that enable you to configure and monitor operating parameters, modify SNMP community names, set SNMP traps, configure switch parameters and configure the 6H123-50 and 6H133-37 ports.

NOTE

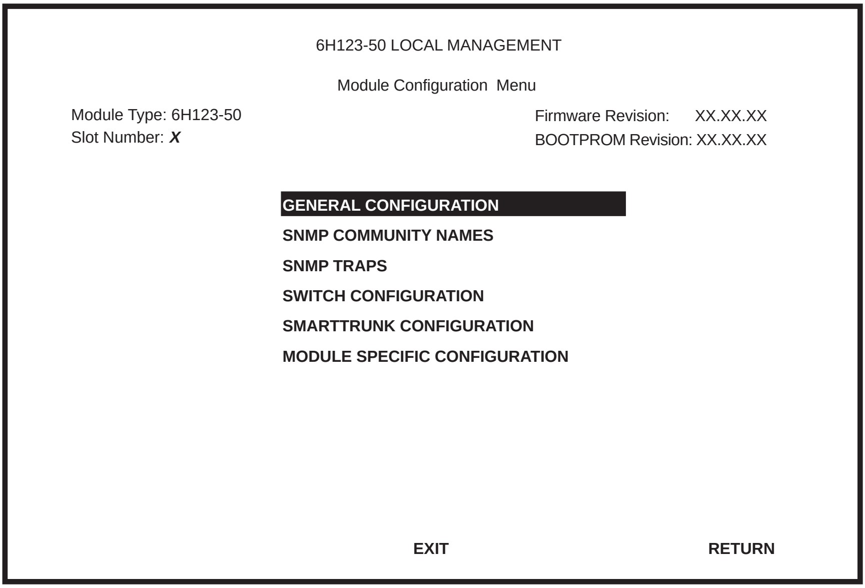
The following menu items on the Module Configuration Menu screen will not display if the operational mode of the module has been set to SECURE FAST VLAN:

SWITCH CONFIGURATION

SMARTTRUNK CONFIGURATION

Section 5.15.9 provides instructions on setting the operational mode.

Access the Module Configuration Menu screen from the Module Menu screen by using the arrow keys to highlight the **MODULE CONFIGURATION** menu item and pressing ENTER. The Module Configuration Menu screen displays.



```
                         6H123-50 LOCAL MANAGEMENT

                          Module Configuration  Menu
Module Type: 6H123-50                                   Firmware Revision:     XX.XX.XX
Slot Number: X                                          BOOTPROM Revision: XX.XX.XX


                    GENERAL CONFIGURATION
                    SNMP COMMUNITY NAMES
                    SNMP TRAPS
                    SWITCH CONFIGURATION
                    SMARTTRUNK CONFIGURATION
                    MODULE SPECIFIC CONFIGURATION




                          EXIT                              RETURN
```

2276_42

Figure 5-17 Module Configuration Menu Screen

The following briefly defines each screen accessible from the Module Configuration Menu screen:

GENERAL CONFIGURATION

The General Configuration screen enables the user to monitor and configure operating parameters for the 6H123-50 and 6H133-37. For details, refer to Section 5.15.

SNMP COMMUNITY NAMES

The SNMP Community Names screen enables the user to enter new, change, or review the community names used as access passwords for Local/Remote management operation. Access is limited based on the password level of the user. For details, refer to Section 5.16.

SNMP TRAPS

The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names. For details, refer to Section 5.17.

SWITCH CONFIGURATION

The Switch Configuration screen provides basic setup options for making a switch operational in the network. For details, refer to Section 5.18.

SMARTTRUNK CONFIGURATION

The SmartTrunk Configuration screen allows the user to logically group interfaces to aggregate high speed uplinks. For details, refer to *SmartTrunk User’s Guide*.

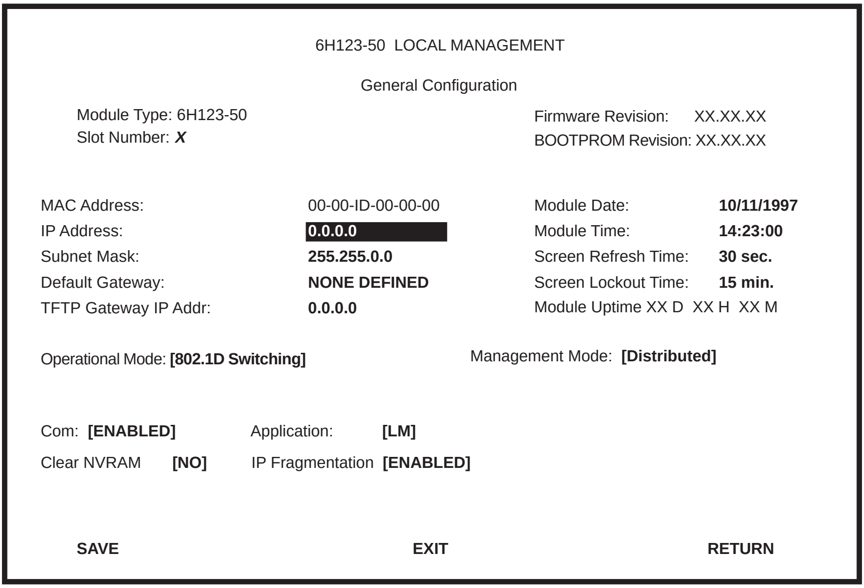
MODULE SPECIFIC CONFIGURATION

The Module Specific Configuration Menu screen enables the user to configure ports or check system resources specific to the 6H123-50 and 6H133-37. For details, refer to Section 5.19.

5.15 GENERAL CONFIGURATION SCREEN

The General Configuration screen, Figure 5-18, enables the user to set the module date and time, IP address and subnet mask, the Default Gateway, the TFTP Gateway IP address, the operation mode, and the COM port configuration. The General Configuration screen also enables the user to Clear NVRAM, set the refresh time, the lockout time and the IP fragmentation.

Access the General Configuration screen from the Module Configuration Menu screen by using the arrow keys to highlight the **GENERAL CONFIGURATION** menu item and pressing ENTER. The General Configuration screen, Figure 5-18, displays.



```
                              6H123-50  LOCAL MANAGEMENT

                                 General Configuration

     Module Type: 6H123-50                               Firmware Revision:     XX.XX.XX
     Slot Number: X                                      BOOTPROM Revision: XX.XX.XX


  MAC Address:                 00-00-ID-00-00-00         Module Date:           10/11/1997
  IP Address:                  0.0.0.0                   Module Time:           14:23:00
  Subnet Mask:                 255.255.0.0               Screen Refresh Time:   30 sec.
  Default Gateway:             NONE DEFINED              Screen Lockout Time:   15 min.
  TFTP Gateway IP Addr:        0.0.0.0                   Module Uptime XX D  XX H  XX M

  Operational Mode: [802.1D Switching]              Management Mode:  [Distributed]


  Com:  [ENABLED]          Application:        [LM]

  Clear NVRAM       [NO]   IP Fragmentation  [ENABLED]


     SAVE                              EXIT                              RETURN
```

2276_15

Figure 5-18 General Configuration Screen

The following briefly defines each General Configuration screen field:

MAC Address (Read-Only)

Displays the physical address of the module.

IP Address (Modifiable)
This display enables the IP address to be set for the 6H123-50 and 6H133-37. To set the IP address, refer to Section 5.15.1.

Subnet Mask (Modifiable)
Displays the subnet mask for the module. A subnet mask “masks out” the network bits of the IP address by setting the bits in the mask to 1 when the network treats the corresponding bits in the IP address as part of the network or subnetwork address, or to 0 if the corresponding bit identifies the host. For details about changing the Subnet Mask from its default value, refer to Section 5.15.2.

Default Gateway (Modifiable)
Displays the default gateway for the 6H123-50 and 6H133-37. This field is not defined until an appropriate value is entered. For details about setting the Default Gateway, refer to Section 5.15.3.

TFTP Gateway IP Addr (Modifiable)
Displays and enables the user to set the TFTP Gateway IP address for the 6H123-50 and 6H133-37. To set the TFTP Gateway IP address, refer to Section 5.15.4.

Module Date (Modifiable)
Contains a value that the module recognizes as the current date. To set a new module date, refer to Section 5.15.5.

Module Time (Modifiable)
Contains a value that the module recognizes as the current time. To enter a new time, refer to Section 5.15.6.

Screen Refresh Time (Modifiable)
Contains the rate at which the screens are updated. This setting determines how frequently (in seconds) information is updated on the screen. To enter a new update time, refer to Section 5.15.7.

Screen Lockout Time (Modifiable)
Contains the maximum number of minutes that the Local Management application displays a module’s screen while awaiting input or action from a user. For example, if the number 5 is entered in this field, the user has up to five minutes to respond to each of the specified module’s Local Management screens.

In this example, after five minutes of “idleness” (no input or action), the terminal “beeps” five times, the Local Management application terminates the session, and the display returns to the Password screen. To enter a new lockout time, refer to Section 5.15.8.

Module Uptime (Read-Only)

Displays the total time that the module has been operating.

Operational Mode (Selectable)

Used to set the 6H123-50 or 6H133-37 so it operates as an 802.1D switch (802.1D SWITCHING), an IEEE 802.1Q switch (802.1Q SWITCHING), or as a Cabletron Systems SecureFast switch (SECURE FAST VLAN).

In all three modes of operation, the 12 connections on each RJ21 port (CONN1 – CONN4 on 6H123-50 or CONN1 – CONN3 on 6H133-37) may be assigned individually to operate at 10 Mbps or 100 Mbps. The connections that share either 10 Mbps or 100 Mbps operation reside on one network (two networks per RJ21 port).

In the 802.1D SWITCHING mode, each of the networks are automatically bridged to each other and to any Fast Ethernet Interface Module in the 6H123-50 or HSIM port(s) in the 6H133-37.

In the 802.1Q SWITCHING mode, the switching function of the device can be increased by creating and maintaining IEEE 802.1Q port based Virtual LANs (VLANs).

In the SECURE FAST VLAN mode, the device acts as a SecureFast switch. With the Cabletron Systems VLAN Manager software, the device is able to increase its switching function by creating and maintaining VLANs.

For details on how to select the Operational Mode, refer to Section 5.15.9.

Management Mode (Toggle)

This field enables the user to select Distributed or Standalone management mode. To select the Management Mode, refer to Figure 5.15.10.

Com (Toggle)

This field enables the user to enable or disable the COM port. The selection toggles between ENABLED and DISABLED. The default is ENABLED. To set up the COM port, refer to Section 5.15.11.

Application (Toggle)
Displays the application set for the COM port. This field enables you to set the application that the COM port supports. The field toggles between LM (Local Management) and UPS (Uninterruptible Power Supply).

The UPS setting enables the COM port to be used to monitor an American Power Conversion Uninterruptible Power Supply (UPS).

The baud rate setting for LM is automatically sensed. For UPS, the baud rate is automatically set to 2400.

For details about configuring the COM port for various applications, refer to Section 5.15.11.

Clear NVRAM (Toggle)
This enables the user to reset NVRAM to the factory default settings. All user-entered parameters, such as IP address and community names are then replaced with 6H123-50 and 6H133-37 default configuration settings. For details, refer to Section 5.15.12.

IP Fragmentation (Toggle)
This field enables the user to enable or disable IP Fragmentation. The default setting for this field is ENABLED. If the 6H123-50 and 6H133-37 will be bridged to an FDDI ring, IP Fragmentation must be enabled. If IP Fragmentation is disabled, all FDDI frames that exceed the maximum Ethernet frame size will be discarded. For details on enabling or disabling IP Fragmentation, refer to Section 5.15.13.

5.15.1 Setting the IP Address

To set the IP address, perform the following steps:

NOTE

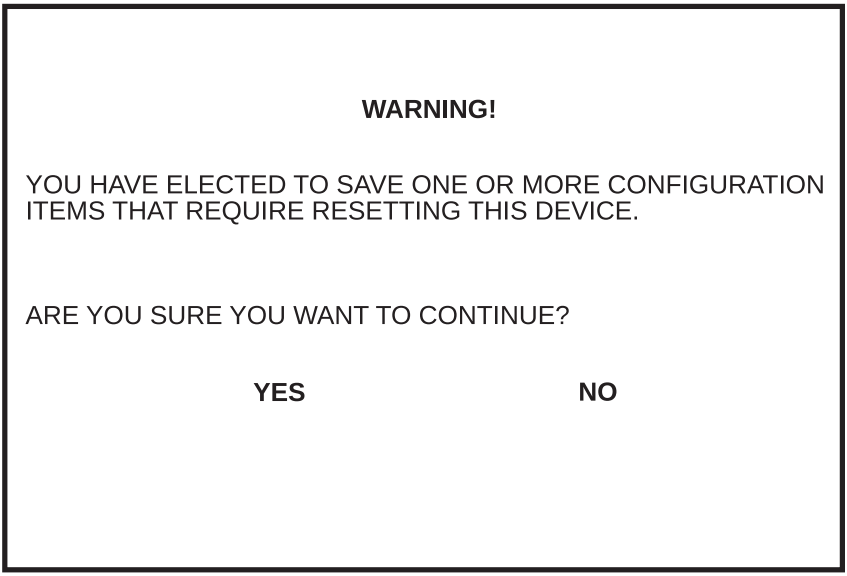
If the 6C105 chassis has been assigned an IP address, it is not necessary to assign an IP address to the 6H123-50 and 6H133-37. All installed modules have the same IP address as the chassis. If a separate IP address for the module is desired, proceed as follows.

1. Use the arrow keys to highlight the **IP Address** field.
2. Enter the IP address into this field using Decimal Dotted Notation (DDN) format.

   For example: 134.141.79.120

3. Press ENTER. If the IP address is a valid format, the cursor returns to the beginning of the IP address field. If the entry is not valid, the Event Message Line displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the IP address field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The Configuration Warning screen, Figure 5-19, displays.



```
                        WARNING!

YOU HAVE ELECTED TO SAVE ONE OR MORE CONFIGURATION
ITEMS THAT REQUIRE RESETTING THIS DEVICE.


ARE YOU SURE YOU WANT TO CONTINUE?

              YES                    NO
```

19601-84

Figure 5-19 Configuration Warning Screen

5. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module resets.

NOTE: The module automatically resets after a new IP address is saved.

5.15.2 Setting the Subnet Mask

If the management workstation that is to receive SNMP traps from the 6H123-50 and 6H133-37 is located on a separate subnet, the subnet mask for the 6H123-50 and 6H133-37 must be changed from its default.

To change the subnet mask from its default, perform the following steps:

NOTE

If the 6C105 chassis has been assigned a subnet mask it is not necessary to assign a subnet mask to the 6H123-50 and 6H133-37. All installed modules have the same subnet mask as the chassis. If a separate subnet mask for the module is desired, proceed as follows.

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the subnet mask into this field using Decimal Dotted Notation (DDN) format.

   For example: 255.255.255.0
3. Press ENTER. If the subnet mask is valid, the cursor returns to the beginning of the Subnet Mask field. If the entry is not valid, the Event Message Line displays “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Subnet Mask field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-19 displays.
5. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.

5.15.3 Setting the Default Gateway

If the SNMP management station is located on a different IP subnet than the 6H123-50 and 6H133-37, a default gateway must be specified. When an SNMP Trap is generated, the 6H123-50 and 6H133-37 sends the Trap to the default gateway.

To set the default gateway, perform the following steps:

1. Use the arrow keys to highlight the **Default Gateway** field.
2. Enter the IP address of the default gateway using the DDN format.

   For example: 134.141.79.121
3. Press ENTER. If the default gateway entered is a valid format, the cursor returns to the beginning of the Default Gateway field. If the entry is not valid, the Event Message Line displays “INVALID DEFAULT GATEWAY OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Default Gateway field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The Event Message Line at the top of the screen displays “SAVED OK”.

5.15.4 Setting the TFTP Gateway IP Address

If the network TFTP server is located on a different IP subnet than the 6H123-50 and 6H133-37, a Gateway IP address should be set. To set the TFTP Gateway IP address, perform the following steps:

1. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
2. Enter the IP address of the TFTP gateway using the DDN format.

   For example: 134.141.80.122
3. Press ENTER. If the TFTP gateway IP address entered is a valid format, the cursor returns to the beginning of the TFTP Gateway IP Address field. If the entry is not valid, the Event Message Line displays “INVALID TFTP GATEWAY IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the TFTP Gateway IP Address field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The Event Message Line at the top of the screen displays “SAVED OK”.

5.15.5 Setting the Module Date

The 6C105 is year 2000 compliant. The Module Date may be set beyond the year 1999. To set the module date, perform the following steps:

NOTE

If the 6C105 chassis has been assigned a chassis date, it is not necessary to assign a module date to the 6H123-50 and 6H133-37. All installed modules recognize the chassis date of the 6C105.

1. Use the arrow keys to highlight the **Module Date** field.
2. Enter the date in this format: MM/DD/YYYY

NOTE

It is not necessary to add separators between month, day, and year numbers. For example, to set the date to 03/17/1997, type “03171997” in the Module Date field.

3. Press ENTER to set the system calendar to the date in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value, but it does refresh the Module Date field with the previous value.

5.15.6 Setting the Module Time

To set the module time, perform the following steps:

NOTE

If the 6C105 chassis has been assigned a chassis time, it is not necessary to assign a module time to the 6H123-50 and 6H133-37. All installed modules recognize the chassis time of the 6C105.

1. Use the arrow keys to highlight the **Module Time** field.
2. Enter the time in this 24-hour format: HH:MM:SS

NOTE

When entering the time in the system time field, separators between hours, minutes, and seconds do not need to be added as long as each entry uses two numeric characters. For example, to set the time to 6:45 A.M., type “064500” in the Module Time field.

3. Press ENTER to set the system clock to the time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value and refreshes the Module Time field with the previous value.

5.15.7 Entering a New Screen Refresh Time

The screen refresh time is set from 3 to 99 seconds with a default of 3 seconds. To set a new screen refresh time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Refresh Time** field.
2. Enter a number from 3 to 99.
3. Press ENTER to set the refresh time to the time entered in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 3 to 99 seconds range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Refresh Time field with the previous value.

5.15.8 Setting the Screen Lockout Time

The screen lockout time can be set from 1 to 30 minutes with a default of 15 minutes. To set a new lockout time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Lockout Time** field.
2. Enter a number from 1 to 30.
3. Press ENTER to set the lockout time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 1 to 30 minutes range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Lockout Time field with the previous value.

5.15.9 Setting the Operational Mode

CAUTION

Before setting the operational mode, ensure that the items contained in this caution are fully understood.

If the module will be configured to operate as a SecureFast switch the following procedures should be performed before setting the operational mode:

The module must be assigned a unique IP address that has been saved (i.e., the module has rebooted and the new IP address is active.)

The Management Mode of the module will automatically be set to [STAND ALONE]. The Management Mode field will no longer display on the General Configuration screen, and the module will no longer support Chassis configuration and Module selection screens. If the module will be a SecureFast switch, distributed management is not allowed.

The module has been assigned SNMP community names from the module SNMP Community Names screen (Section 5.16). In STAND ALONE management mode, the module does not use the community names of the 6C105 chassis.

To set the Operational Mode, proceed as follows:

1. Use arrow keys to highlight the **Operational Mode** field.
2. Press the SPACE bar to step to the appropriate operational mode, (**802.1D SWITCHING**, **802.1Q SWITCHING** or **SecureFast VLAN**).
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER. The Configuration Warning screen shown back in Figure 5-19 displays.

NOTE

If the 6H123-50 and 6H133-37 have been set to **SecureFast VLAN**, refer to your SecureFast documentation set to configure the devices for this type of operation.

4. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.

NOTE

Upon saving the new operational mode, the module reboots.

If the 6H123-50 and 6H133-37 have been set to 802.1Q SWITCHING, refer to the *Port Based VLAN User's Guide* to configure the devices for this type of operation.

If the 6H123-50 and 6H133-37 have been set to SECURE FAST VLAN, refer to your SecureFast documentation set to configure the devices for this type of operation.

5.15.10 Setting the Management Mode

To set the Management mode, perform the following steps:

NOTE

Upon saving the new Management Mode, the module will reboot.

If the module will be set to STAND ALONE, ensure the following procedures have been completed:

The module has been assigned a unique IP address that has been saved (i.e., the module has rebooted and the new IP address is active.)

The module has been assigned SNMP community names from the module SNMP Community Names screen (Section 5.16). In STAND ALONE management mode, the module does not use the community names of the 6C105 chassis.

1. Use the arrow keys to highlight the **Management Mode** field:
2. Use the SPACE bar to toggle the options **DISTRIBUTED** or **STAND ALONE** until the desired mode displays.
3. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown back in Figure 5-19 displays.
4. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.

5.15.11 Configuring the COM Port

CAUTION

Before altering the COM port settings, ensure that a valid IP address is set for the module or chassis. (Refer to Section 5.15.1.) Read this entire COM port configuration section before changing the settings of the COM port.

The 6H123-50 and 6H133-37 COM ports support the following applications:

- Local Management connections
- American Power Conversion Uninterruptible Power Supply (UPS) connections

To configure the COM port, proceed as follows:

1. Use the arrow keys to highlight the **Com** field.

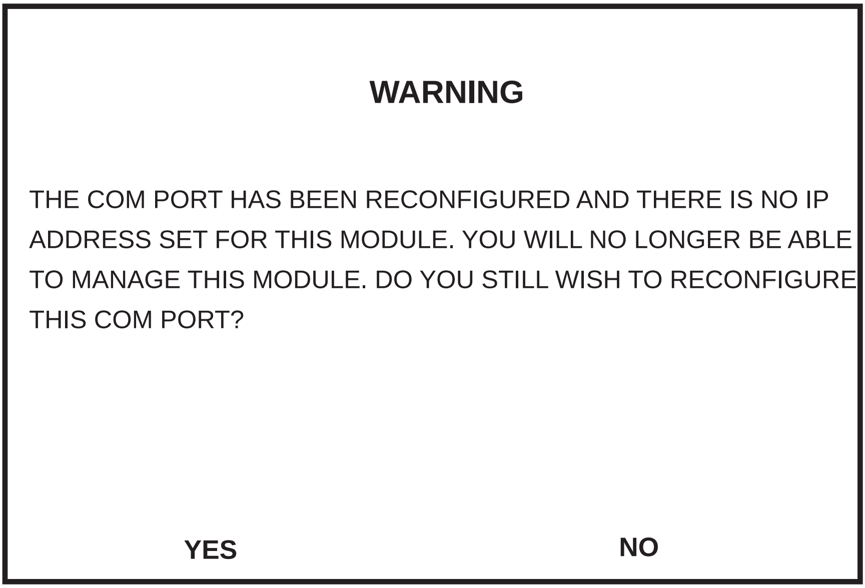
CAUTION

Do **NOT** disable or alter the settings of the COM port while operating the current Local Management connection through a terminal. Altering the COM port settings disconnects the Local Management terminal from the port, and ends the Local Management session.

2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**. The COM port must be **ENABLED** if it is to be used for Local Management or UPS applications. Select **DISABLED** if you wish to disable the COM port for additional module security.

CAUTION

If the COM port is reconfigured without a valid IP address set on the module or chassis, the message shown in Figure 5-20 displays. Do not continue unless you fully understand the outcome of the action.



WARNING

THE COM PORT HAS BEEN RECONFIGURED AND THERE IS NO IP ADDRESS SET FOR THIS MODULE. YOU WILL NO LONGER BE ABLE TO MANAGE THIS MODULE. DO YOU STILL WISH TO RECONFIGURE THIS COM PORT?

174252

Figure 5-20 COM Port Warning Screen

NOTE

If the 6C105 chassis has been configured with a valid IP address this screen does not appear. When the chassis is assigned a valid IP address all the interface modules installed share this same address.

3. Use the arrow keys to highlight **YES**. Press ENTER.
4. If you **ENABLED** the port, proceed to Section 5.15.11.1. If you **DISABLED** the port, use the arrow keys to highlight **SAVE** at the bottom of the screen, then press ENTER. When the message “SAVED OK” displays, the edits are saved.

CAUTION

Exiting without saving causes the message “NOT SAVED -- PRESS SAVE TO KEEP CHANGES” to appear. Exiting without saving causes all edits to be lost.

5.15.11.1 Changing the COM Port Application

After enabling the COM port as described in Section 5.15.11, you can select one of the applications supported by the COM port: LM or UPS. The default application is LM.

To change the COM port application:

1. Use the arrow keys to highlight the **Application** field.
2. Use the SPACE bar or BACKSPACE to step through the available settings until the operation you require displays. Table 5-3 lists the available settings and their corresponding applications.

Table 5-3. COM Port Application Settings

Setting	Application
LM	Local Management Session
UPS	APC Power Supply SNMP Proxy

3. Press ENTER to accept the application.
4. Use the arrow keys to highlight **SAVE** at the bottom of the screen, then press the ENTER key.

CAUTION

When the COM port is configured to perform the UPS application, all future Local Management connections must be made by establishing a Telnet connection to the module. Ensure that the module has a valid IP address before saving changes to the COM port application. If the module does not have a valid IP address and the changes are saved, refer to Appendix C for instructions on clearing NVRAM in order to reestablish COM port communications.

5. When the message “SAVED OK” appears, the edits made are saved.

5.15.12 Clearing NVRAM

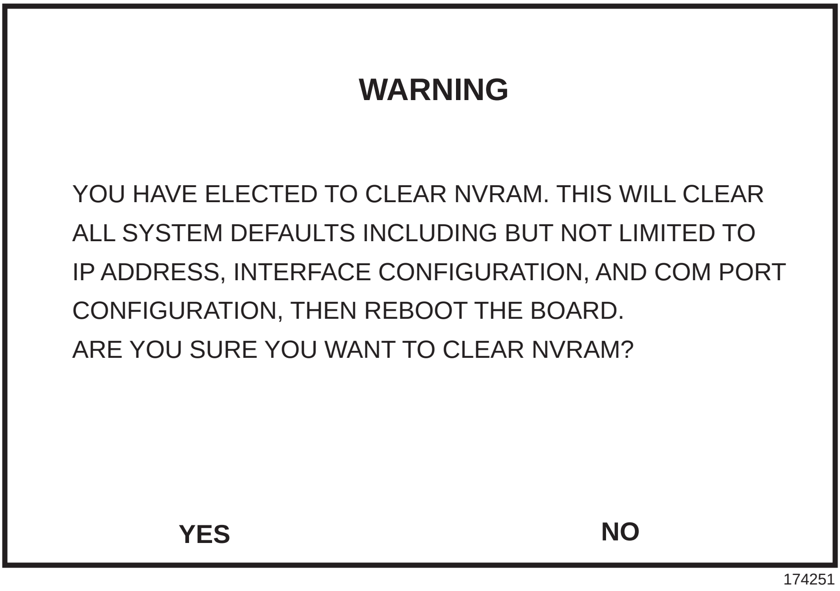
CAUTION

Clearing NVRAM results in the loss of all user-entered parameters. Do not proceed unless you fully understand this procedure.

Clearing NVRAM enables the user to clear all user-entered parameters, such as IP address and Community Names from NVRAM.

Clear NVRAM as follows:

1. Use the arrow keys to highlight the **Clear NVRAM** field.
2. Use the SPACE bar to toggle the field to **YES**.
3. Use the arrow keys to highlight **SAVE** at the bottom of the screen.
4. Press ENTER. The warning shown in Figure 5-21 displays.



WARNING

YOU HAVE ELECTED TO CLEAR NVRAM. THIS WILL CLEAR ALL SYSTEM DEFAULTS INCLUDING BUT NOT LIMITED TO IP ADDRESS, INTERFACE CONFIGURATION, AND COM PORT CONFIGURATION, THEN REBOOT THE BOARD.
ARE YOU SURE YOU WANT TO CLEAR NVRAM?

Figure 5-21 Clear NVRAM Warning Screen

5. Use the arrow keys to highlight **YES** and press ENTER. The message “CLEARING NVRAM. REBOOT IN PROGRESS...” displays.

The 6H123-50 and 6H133-37 clear NVRAM and reboot. All user-entered parameters default to factory settings.

5.15.13 Enabling/Disabling IP Fragmentation

CAUTION If the 6H133-37 is being bridged to an FDDI ring (for example, via an HSIM-F6 installed in the 6H133-37) IP Fragmentation should be enabled. If IP Fragmentation is disabled, all FDDI frames that exceed the maximum Ethernet frame size will be discarded.

To enable or disable IP fragmentation, proceed as follows.

1. Use the arrow keys to highlight the **IP Fragmentation** field.
2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**.
3. Use the arrow keys to highlight the **SAVE** command.
4. Press ENTER. The Event Message Line at the top of the screen displays “SAVED OK”.

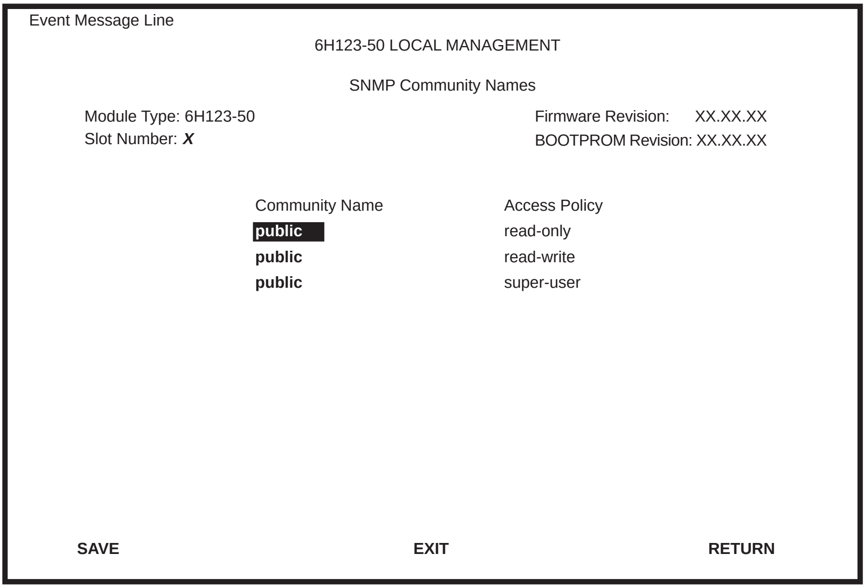
5.16 SNMP COMMUNITY NAMES SCREEN

The SNMP Community Names screen enables the user to set Local/Remote Management community names. Community names act as passwords to Local/Remote Management and are agents of security access to the 6H123-50 and 6H133-37. Access to the 6H123-50 and 6H133-37 is controlled by enacting any of three different levels of security authorization (read-only, read-write, and super-user).

NOTE If the 6C105 has been assigned community names, it is not necessary to assign community names to the individual modules installed in the chassis unless the user wishes to limit access to 6C105 chassis screens by assigning different community names to the module. When this is done access is limited to the screens specific to the module to which the terminal is attached and the Local Management session begins at the Module Menu screen. See Section 5.13.

Super-User access gives the user full management privileges, allows existing passwords to be changed, and all modifiable MIB objects for the Cabletron Container MIB and Internet MIB-II to be accessed.

Access the SNMP Community Names screen from the Module Configuration Menu screen by using the arrow keys to highlight the **SNMP COMMUNITY NAMES** menu item and pressing ENTER. The SNMP Community Names screen, Figure 5-22, displays.



```
Event Message Line
                         6H123-50 LOCAL MANAGEMENT

                           SNMP Community Names

   Module Type: 6H123-50                     Firmware Revision:     XX.XX.XX
   Slot Number: X                            BOOTPROM Revision: XX.XX.XX


                 Community Name          Access Policy
                 public                  read-only
                 public                  read-write
                 public                  super-user









   SAVE                        EXIT                          RETURN
```

2276_16

Figure 5-22 SNMP Community Names Screen

The following defines each SNMP Community Names screen field:

Community Name (Modifiable)

Displays the user-defined name through which a user accesses 6H123-50 and 6H133-37 management. Any community name assigned here acts as a password to Local/Remote Management.

Access Policy (Read-Only)

Indicates the access accorded each community name. Possible selections are as follows:

read-only
This community name allows read-only access to the 6H123-50 and 6H133-37 MIB objects, and excludes access to security-protected fields of read-write or super-user authorization.

read-write
This community name allows read and write access to the 6H123-50 and 6H133-37 MIB objects, excluding security protected fields for super-user access only.

super-user
This community name permits read-write access to the 6H123-50 and 6H133-37 MIB objects and allows the user to change all modifiable parameters including community names, IP addresses, traps, and SNMP objects.

5.16.1 Establishing Community Names

The password used to access Local Management at the Password Screen must have super user access in order to view and edit the SNMP Community Names screen. Using a password with read-only or read-write access does not enable the user to view or edit the SNMP Community Names screen.

NOTE

Any community name assigned in the SNMP Community Names screen is a password to its corresponding level of access to Local/Remote Management. The community name assigned super user access is the only one that gives the user complete access to Local/Remote Management.

To establish community names, proceed as follows:

1. Use the arrow keys to highlight the **Community Name** field adjacent to the selected access level.
2. Enter the password in the field (maximum 31 characters).
3. Press ENTER.

4. Repeat steps 1 through 3 to modify the other community names.

5. Use the arrow keys to highlight **SAVE** at the bottom of the screen and press ENTER. The message “SAVED OK” displays. The community names are saved to memory and their access modes implemented.

NOTE

Exiting without saving causes a “NOT SAVED?” message to display. Edits are lost if they are not saved before exiting.

6. To exit the screen, use the arrow keys to highlight **RETURN** and press ENTER.

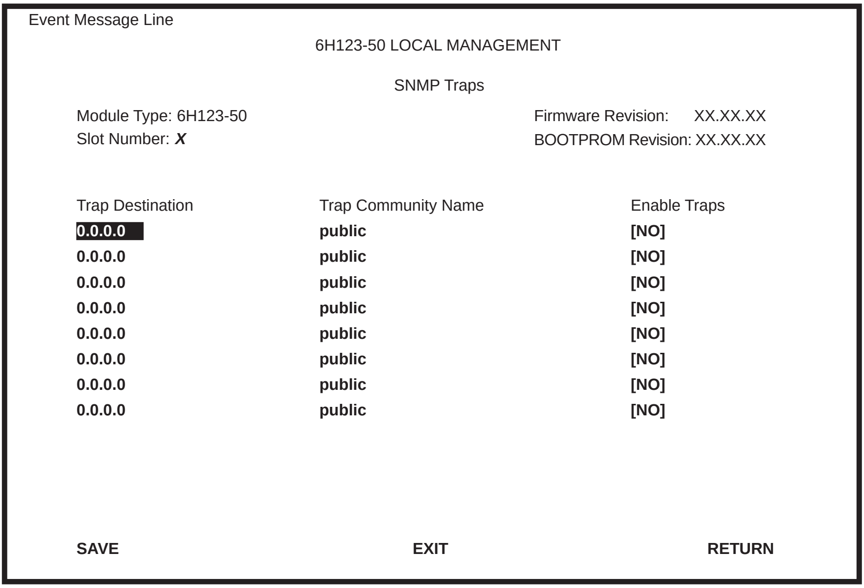
5.17 SNMP TRAPS SCREEN

Since the 6H123-50 and 6H133-37 are SNMP compliant devices, they can send messages to multiple Network Management Stations to alert users of status changes. The SNMP Traps screen is shown in Figure 5-23.

NOTE

It is only necessary to assign SNMP traps if the user desires the traps to be sent to different addresses than those assigned in Section 5.9, which details how to set SNMP Traps for the 6C105 chassis.

Access the SNMP Traps screen from the Module Configuration Menu screen by using the arrow keys to highlight the **SNMP TRAPS** menu item and pressing ENTER. The SNMP Traps screen displays.



```
Event Message Line
                              6H123-50 LOCAL MANAGEMENT

                                     SNMP Traps

     Module Type: 6H123-50                            Firmware Revision:     XX.XX.XX
     Slot Number: X                                   BOOTPROM Revision: XX.XX.XX


     Trap Destination         Trap Community Name          Enable Traps
     0.0.0.0                  public                       [NO]
     0.0.0.0                  public                       [NO]
     0.0.0.0                  public                       [NO]
     0.0.0.0                  public                       [NO]
     0.0.0.0                  public                       [NO]
     0.0.0.0                  public                       [NO]
     0.0.0.0                  public                       [NO]
     0.0.0.0                  public                       [NO]




     SAVE                               EXIT                          RETURN
```

2276_17

Figure 5-23 SNMP Traps Screen

The following defines each field of the SNMP Traps screen.

Trap Destination (Modifiable)

Indicates the IP address of the workstation to receive trap alarms. Up to eight different destinations can be defined.

Trap Community Name (Read-only)
Displays the Community Name included in the trap message sent to the Network Management Station with the associated IP address.

Enable Traps (Toggle)
Enables transmission of the traps to the network management station with the associated IP address. This field toggles between **YES** and **NO**.

5.17.1 Configuring the Trap Table

To configure the Trap table, proceed as follows:

1. Using the arrow keys, highlight the appropriate **Trap Destination** field.
2. Enter the IP Address of the workstation that is to receive traps. IP address entries must follow the DDN format.

   For example: 134.141.79.121
3. Press ENTER. If an invalid entry is entered “INVALID IP ENTERED” displays in the Event Message Line.
4. Using the arrow keys, highlight the **Trap Community Name** field. Enter the community name.
5. Press ENTER.
6. Using the arrow keys, highlight the **Enable Traps** field. Press the SPACE bar to choose either **YES** (send alarms from the module to the workstation), or **NO** (prevent alarms from being sent).
7. Using the arrow keys, highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays on the screen.

NOTE

Exiting without saving causes a “NOT SAVED?” message to appear above the **SAVE** command. Edits are lost if they are not saved before exiting.

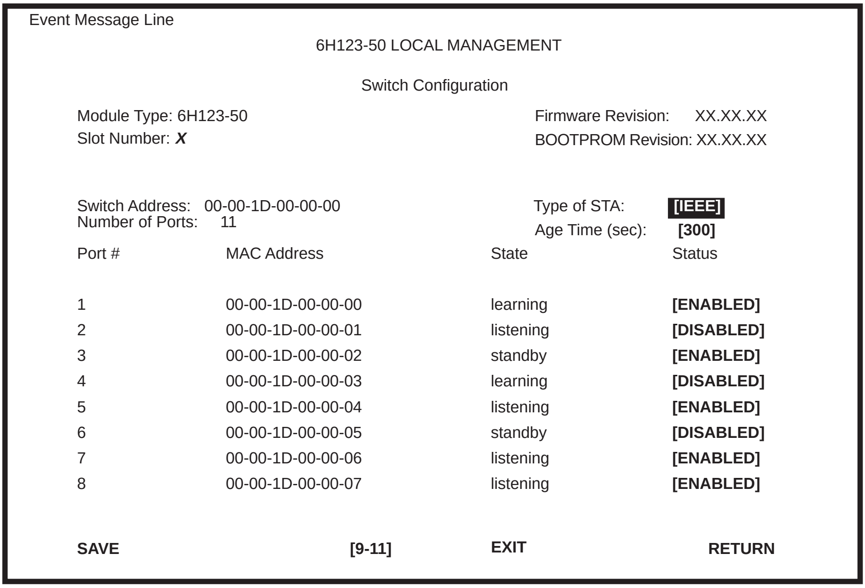
8. To exit the screen, use the arrow keys to highlight **RETURN** and press ENTER.

The designated workstations now receive traps from the 6H123-50 and 6H133-37.

5.18 SWITCH CONFIGURATION SCREEN

The Switch Configuration screen, Figure 5-24, provides the basic setup options to customize switch operation in your network.

Access the Switch Configuration screen from the Module Configuration Menu screen by using the arrow keys to highlight the **SWITCH CONFIGURATION** menu item and pressing ENTER. The Switch Configuration screen, Figure 5-24, displays.



```
Event Message Line
                              6H123-50 LOCAL MANAGEMENT

                                 Switch Configuration

     Module Type: 6H123-50                              Firmware Revision:     XX.XX.XX
     Slot Number: X                                     BOOTPROM Revision: XX.XX.XX


     Switch Address:   00-00-1D-00-00-00                Type of STA:        [IEEE]
     Number of Ports:      11                           Age Time (sec):      [300]
     Port #            MAC Address               State               Status


     1                 00-00-1D-00-00-00         learning            [ENABLED]
     2                 00-00-1D-00-00-01         listening           [DISABLED]
     3                 00-00-1D-00-00-02         standby             [ENABLED]
     4                 00-00-1D-00-00-03         learning            [DISABLED]
     5                 00-00-1D-00-00-04         listening           [ENABLED]
     6                 00-00-1D-00-00-05         standby             [DISABLED]
     7                 00-00-1D-00-00-06         listening           [ENABLED]
     8                 00-00-1D-00-00-07         listening           [ENABLED]


     SAVE                        [9-11]          EXIT                     RETURN
```

2276_18

Figure 5-24 Switch Configuration Screen

NOTE

The Switch Configuration screen will not be available if the operational mode of the module has been set to SECURE FAST VLAN. This screen may only be used by modules configured to operate as 802.1D or 802.1Q switches.

Depending on the optional interfaces installed and if the device is a 6H123-50 or 6H133-37, there can be 10 or 7 switched or network ports. Table 5-4 shows the CONN/port organization.

Table 5-4 CONN/Port Organization

6H123-50	6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 4 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	HSIM = Port 7
Fast Ethernet Slot 5 = Port 9	
Fast Ethernet Slot 6 = Port 10	

The following describes each field of the Switch Configuration screen.

Switch Address (Read-Only)

Displays the MAC address of the switch.

Number of Ports (Read-Only)

Displays the total number of switched ports on the module.

NOTE

Each Ethernet and Fast Ethernet network are considered single switched ports.

Type of STA (Selectable)

Enables the user to set the method that switches use to decide which switch is the controlling (Root) switch when two or more switches exist in parallel (Spanning Tree Algorithm). Valid entries include IEEE, DEC, and NONE. To set the STA, refer to Section 5.18.1.

Age Time (Modifiable)

Enables the user to set the amount of time (in seconds) the 6H123-50 and 6H133-37 keep an address in its switch table before discarding it. The modules will discard an address from their switch table if they do not receive a valid frame from the applicable address in the amount of time specified in the Age Time field. To change the Age Time field from the default value of 300 seconds, refer to Section 5.18.2.

Port # (Read-Only)

Lists each switch port on the module.

MAC Address (Read-Only)

Displays the hardware address assigned to each listed port.

State (Read-Only)

Disabled: Management disabled this interface. No traffic is received or forwarded while the interface is disabled.

Listening: The switch is not adding information to the Transparent Database. The switch is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move from the learning to the forwarding state.

Learning: The switch is learning the network address of this interface. The switch enters the learning state when the Transparent Database is created (during start-up or after being deleted), or when the Spanning Tree Algorithm detects a network topology change.

Forwarding: The switch is operating and this interface is forwarding traffic.

Blocking: This interface will not forward any traffic through the switch because a loop condition has been detected by the STA.

Status (Toggle)

Allows the user to disable or enable a port by setting the status of the listed interface to either ENABLED or DISABLED. To set the port status, refer to Section 5.18.3.

[1-8] or **[9-11]** (Navigation Key)
When the Switch Configuration screen displays, the current port configuration information is displayed for the first 8 ports. This field allow the user to step to a second screen (if 6H123-50) to display the information for ports 9 through 11. Depending on the current screen displayed, the user can navigate back and forth by highlighting the **[1-8]** or **[9-11]** field and pressing ENTER.

5.18.1 Setting the STA

The Spanning Tree Algorithm (STA) setting enables the user to set the method that the switches use to decide which is the controller (Root) switch when two or more switches are in parallel. The available selections are IEEE, DEC, and NONE.

To set the STA, proceed as follows:

1. Use the arrow keys to highlight the **Type of STA** field.
2. Use the SPACE bar to step to the appropriate setting of **IEEE**, **DEC**, or **NONE**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.18.2 Setting the Age Time

To set the Age Time, proceed as follows:

1. Use the arrow keys to highlight the **Age Time** field.
2. Enter the desired Age Time in increments of 10. The available Age Time range is 10 to 1,000,000 seconds with the default value being 300 seconds.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.18.3 Setting (Enabling or Disabling) the Port Status

To set the status of an interface (port), proceed as follows:

1. Use the arrow keys to highlight the **Status** field of the port.
2. Use the SPACE bar to toggle to either **ENABLED** or **DISABLED**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.19 MODULE SPECIFIC CONFIGURATION SCREEN

The Module Specific Configuration screen, Figure 5-25, enables the user to select screens to configure ports or check system resources specific to the 6H123-50 and 6H133-37.

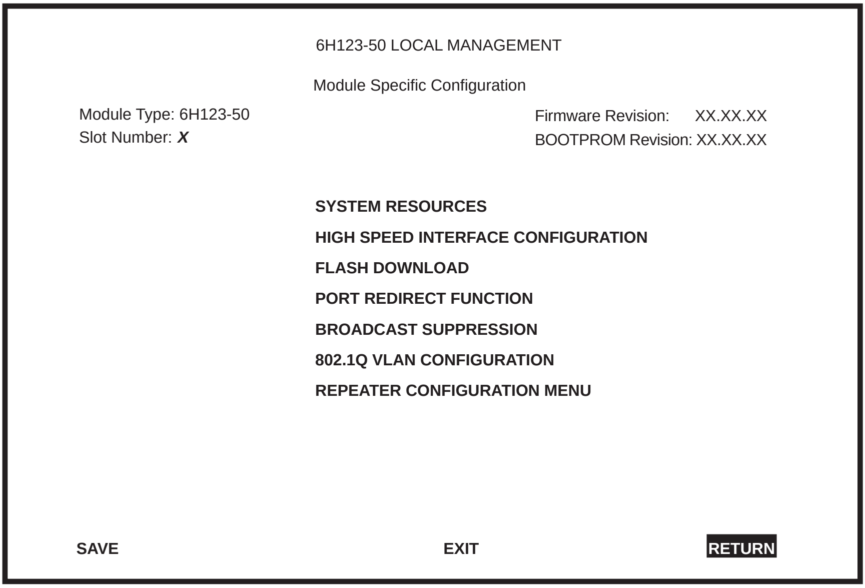
NOTE

The PORT REDIRECT FUNCTION menu item on the Device Specific Configuration Menu screen does not display if the operational mode of the device is set to 802.1Q SWITCHING.

The PORT REDIRECT FUNCTION and BROADCAST SUPPRESSION menu items do not display if the operational mode is set to SECURE FAST VLAN.

Section 5.15.9 provides instructions on setting the operational mode.

Access the Module Specific Configuration screen from the Module Configuration Menu screen by using the arrow keys to highlight the **MODULE SPECIFIC CONFIGURATION** menu item and pressing ENTER. The Module Specific Configuration screen displays.



```
                         6H123-50 LOCAL MANAGEMENT

                        Module Specific Configuration
Module Type: 6H123-50                               Firmware Revision:    XX.XX.XX
Slot Number: X                                      BOOTPROM Revision: XX.XX.XX


                         SYSTEM RESOURCES
                         HIGH SPEED INTERFACE CONFIGURATION
                         FLASH DOWNLOAD
                         PORT REDIRECT FUNCTION
                         BROADCAST SUPPRESSION
                         802.1Q VLAN CONFIGURATION
                         REPEATER CONFIGURATION MENU




SAVE                              EXIT                              RETURN
```

2276_20

Figure 5-25 Module Specific Configuration Screen

The following defines each field of the Module Specific Configuration screen:

SYSTEM RESOURCES

The System Resources screen displays the amount of FLASH memory, DRAM, and NVRAM installed, details how much memory is available and provides information on 6H123-50 and 6H133-37 operation. For details, refer to Section 5.20.

HIGH SPEED INTERFACE CONFIGURATION

The High Speed Interface Configuration screen indicates which Fast Ethernet Interface Modules are installed in slots 5 and 6 of the 6H123-50, their current operating mode, and if the ports are linked. This screen also allows the Auto-Negotiation and Advertised Ability features to be enabled or disabled. For details, refer to Section 5.21.

The High Speed Interface Configuration screen for the 6H133-37 enables management of an installed HSIM. For details, refer to the applicable HSIM user's guide.

FLASH DOWNLOAD

The FLASH Download screen enables the user to download a new image file from a TFTP server. For details, refer to Section 5.22.

PORT REDIRECT FUNCTION

The Port Redirect Function screen enables the user to redirect traffic from one or multiple interfaces to a specific destination interface. For details, refer to Section 5.23.

BROADCAST SUPPRESSION

The Broadcast Suppression screen enables the user to set a desired limit of receive broadcast frames per port per second. For details, refer to Section 5.24.

802.1Q VLAN CONFIGURATION

This menu item only displays if the module is configured as an 802.1Q switch and accesses the VLAN Main Menu screen. The 802.1Q VLAN configuration screen enables the user to create VLANs, add and delete ports for VLANs and set operational parameters. For more information refer to the Cabletron Systems *Port Based VLAN User's Guide*.

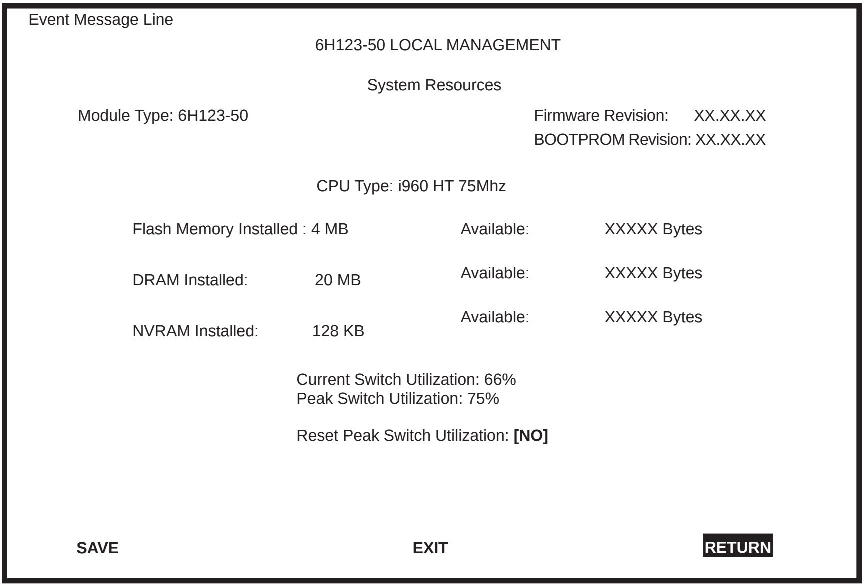
REPEATER CONFIGURATION

This menu item is used to select the Repeater Port Configuration Menu screen, which provides access to the Security screens: Repeater Port Configuration, Module Level Security Configuration, and Port Level Security Configuration. For details refer to Section 5.26.

5.20 SYSTEM RESOURCES SCREEN

The System Resources screen, Figure 5-26, provides information concerning the processor used in the 6H123-50 and 6H133-37 and the amount of FLASH memory, DRAM, and NVRAM that are installed and how much of that memory is available.

Access the System Resources screen from the Module Specific Configuration Menu screen by using the arrow keys to highlight the **SYSTEM RESOURCES** menu item and pressing ENTER. The System Resources screen displays.



```
Event Message Line
                                6H123-50 LOCAL MANAGEMENT

                                    System Resources
     Module Type: 6H123-50                              Firmware Revision:    XX.XX.XX
                                                        BOOTPROM Revision: XX.XX.XX

                                CPU Type: i960 HT 75Mhz

          Flash Memory Installed : 4 MB          Available:         XXXXX Bytes

          DRAM Installed:          20 MB         Available:         XXXXX Bytes

          NVRAM Installed:         128 KB        Available:         XXXXX Bytes

                              Current Switch Utilization: 66%
                              Peak Switch Utilization: 75%

                              Reset Peak Switch Utilization: [NO]


     SAVE                           EXIT                            RETURN
```

Figure 5-26 System Resources Screen

The following briefly defines each field of the System Resources screen.

CPU Type (Read-Only)

Indicates the microprocessor used in the 6H123-50 and 6H133-37.

Flash Memory Installed (Read-Only)

Indicates the amount of FLASH memory installed in the 6H123-50 and 6H133-37 and how much is currently available.

DRAM Installed (Read-Only)

Indicates the amount of DRAM installed in the 6H123-50 and 6H133-37 and how much of it is currently available.

NVRAM Installed (Read-Only)

Indicates the amount of NVRAM installed in the 6H123-50 and 6H133-37 and how much of it is currently available.

Current Switch Utilization (Read-Only)

Shows how much (percentage of capacity) the 6H123-50 and 6H133-37 is currently being used.

Peak Switch Utilization (Read-Only)
Shows the peak percentage of maximum switching capacity, since last reset.

Reset Peak Switch Utilization (Toggle)
Enables the user to reset the Peak Switch Utilization field. The switch may be set to either YES or NO as described in Section 5.20.1. YES resets the Peak Switch Utilization field to the current system traffic.

5.20.1 Setting the Reset Peak Utilization

To set the Reset Peak Utilization field to YES or NO, proceed as follows:

1. Use the arrow keys to highlight the **Reset Peak Utilization** field.
2. Press the SPACE bar to select **YES** or **NO**.
3. Use the arrows keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.21 HIGH SPEED INTERFACE CONFIGURATION SCREEN (6H123-50 ONLY)

NOTE

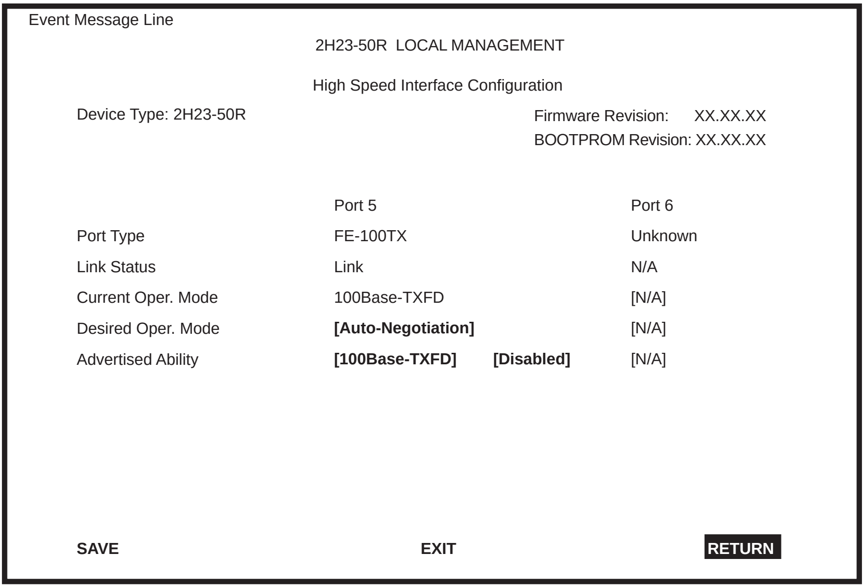
When the HIGH SPEED CONFIGURATION MENU item is selected for the 6H133-37, the applicable HSIM Setup screen displays. Refer to the HSIM user’s guide to set operating parameters for the HSIM installed in the 6H133-37.

To access the High Speed Interface Configuration Menu screen from the Device Specific Configuration Menu screen, use the arrow keys to highlight the **HIGH SPEED INTERFACE CONFIGURATION** menu item and press ENTER. The High Speed Interface Configuration screen, Figure 5-27, displays.

NOTE

The High Speed Interface Configuration screen, Figure 5-27, applies only to slots 5 and 6 of the 6H123-50. This screen supports the FE-100TX, FE-100FX, and FE-100F3 Fast Ethernet Interface Modules that operate at 100 Mbps.

The High Speed Interface Configuration screen displays the types of interfaces installed in slots 5 and 6, their current operating mode, and indicates if the ports are linked. This screen also allows the user to enable or disable Auto-Negotiation and set the Advertised Ability.



```
Event Message Line
                              2H23-50R  LOCAL MANAGEMENT

                           High Speed Interface Configuration
     Device Type: 2H23-50R                          Firmware Revision:     XX.XX.XX
                                                    BOOTPROM Revision: XX.XX.XX


                              Port 5                          Port 6
     Port Type                FE-100TX                        Unknown
     Link Status              Link                            N/A
     Current Oper. Mode       100Base-TXFD                    [N/A]
     Desired Oper. Mode       [Auto-Negotiation]              [N/A]
     Advertised Ability       [100Base-TXFD]    [Disabled]    [N/A]
```

22861-24

Figure 5-27 High Speed Interface Configuration Screen

The following briefly defines each field of the High Speed Interface Configuration screen.

Port Type (Read-only)

Displays the type of interface (FE-100FX, FE-100TX, FE-100F3, or Unknown) installed in slots 5 and 6. Figure 5-27 shows that there is an FE-100TX interface installed in slot 5 and no interface (indicated by Unknown) in slot 6.

Link Status (Read-only)

Indicates whether or not there is a physical connection from this port to another 10BASE-T or 100BASE-TX/FX device. One of the following values displays:

- **Link –** There is a link signal present and a valid physical connection to another device.
- **No Link –** There is no link signal present and no valid physical connection to another device.

Current Oper. Mode (Read-only)

This field displays the current operating mode of slots 5 and 6. Depending on whether a 100BASE-FX or 100BASE-TX Fast Ethernet Interface Module is installed, this field displays the following:

- With a 100BASE-FX interface: 100Base-FX, 100Base-FXFD (full duplex), or N/A when the slot is empty.
- With a 100BASE-TX interface: Unknown, 10Base-T, 10Base-TFD (full duplex), 100Base-TX, 100Base-TXFD (full duplex), or N/A when the slot is empty.

Desired Oper. Mode (Selectable)

This field allows the user to select the desired operational mode for an interface in slot 5 or 6. The field toggles between 100Base-FX and 100Base-FXFD (full duplex) when an FE-100FX or FE-100F3 is installed. Section 5.21.1 describes how to configure a port with an FE-100FX or FE-100F3.

NOTE

In normal operation, the port with an FE-100TX installed automatically establishes a link with the device at the other end of the segment without requiring user setup. However, Local Management provides the user with the option of manually configuring that port.

If an FE-100TX is installed, the field steps to Auto-Negotiation, 10Base-T, 10Base-TFD (full duplex), 100Base-TX, and 100Base-TXFD (full duplex). In normal operation, the port with an FE-100TX installed is capable of auto-negotiating the operational mode and no further user setup is required. Section 5.21.2 describes how to manually configure an FE-100TX.

In Auto-Negotiation, the FE-100TX negotiates to the highest common denominator of the two interfaces. The order of priority of negotiation is 100Base-TXFD, 100Base-TX, 10Base-TFD, and 10Base-T.

Advertised Ability (Selectable)
During auto-negotiation, the FE-100TX informs the device at the other end of the segment about its capabilities. The capabilities of a slot (5 or 6) with an FE-100TX installed are 10Base-T, 10Base-TFD (full duplex mode), 100Base-TX and 100Base-TXFD (full duplex mode). In normal operation, with all capabilities enabled, the FE-100TX “advertises” that it has the ability to operate in any mode. The Network Manager may choose to set up the port so that only a portion of the available capabilities are advertised and the others are disabled. For example, only 100Base-TX and 100Base-TXFD might be enabled so that only devices that operate at 100 Mbps can communicate with that port. Section 5.21.2.2 describes how to enable or disable advertised modes.

5.21.1 Configuring an FE-100FX or FE-100F3

When an FE-100FX or FE-100F3 is installed in slot 5 or 6, it must be manually set to operate in the same technology as the device at the other end of the connected segment. Section 5.21.1.1 provides instructions for manually configuring the port slot with an FE-100FX or FE-100F3 interface.

5.21.1.1 Setting the FE-100FX or FE-100F3 Operational Mode

Use the Desired Oper. Mode field to set the active technology. This field toggles between 100Base-FX and 100Base-FXFD (full duplex). To set the active technology through Local Management, proceed as follows:

1. Use the arrow keys to highlight the **Desired Oper. Mode** field.
2. Use the SPACE bar to select **100Base-FX** or **100Base-FXFD** (full duplex).
3. Press ENTER. The port now operates in the chosen mode.
4. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “SAVED OK” displays and Local Management saves the changes to memory.

5.21.2 Configuring an FE-100TX

In normal operation, a slot (5 or 6) with an FE-100TX interface automatically establishes a link with the device at the other end of the segment and no user setup is required. Section 5.21.2.1 and Section 5.21.2.2 provide instructions for manually configuring the port with an FE-100TX installed.

5.21.2.1 Setting the FE-100TX Operational Mode

Use the Desired Oper. Mode field to set the active technology. This field steps between Auto-Negotiation, 10Base-T, 10Base-TFD (full duplex), 100Base-TX, and 100Base-TXFD (full duplex). If Auto-Negotiation is selected, the FE-100TX automatically sets the active technology. To manually set the active technology through Local Management, proceed as follows:

1. Use the arrow keys to highlight the **Desired Oper. Mode** field.
2. Use the SPACE bar to select the desired mode. Press ENTER. If any mode other than Auto-Negotiation is selected, the port only operates in the chosen mode and Auto-Negotiation is disabled.
3. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “SAVED OK” displays and Local Management saves the changes to memory. The selected mode is displayed in both the Desired Operational Mode field and the Current Operational Mode field.

5.21.2.2 Setting the FE-100TX Advertised Ability

In normal operation, a slot (5 or 6) with an FE-100TX auto-negotiates to the highest speed possible. Under some circumstances, the Network Administrator may want the slot to advertise only some of the available modes. The Advertised Ability field provides the capability to set those modes. This field steps to 10Base-T, 10Base-TFD (full duplex), 100Base-TX, and 100Base-TXFD (full duplex). To set the advertised ability, proceed as follows:

1. Use the arrow keys to highlight the **Desired Oper. Mode** field.
2. Use the SPACE bar to select the desired mode.

3. Use the LEFT-ARROW key to move back to the **Advertised Ability** selection and use the SPACE bar to select the next mode to enable or disable.
4. Use the RIGHT-ARROW key to move across to the **Enabled/Disabled** field to the right of the selection.
5. Use the SPACE bar to select **Enabled** or **Disabled**. Press ENTER. Continue this process until you have completed enabling or disabling the advertised modes.
6. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message "SAVED OK" displays and Local Management saves the changes to memory.

5.22 FLASH DOWNLOAD SCREEN

The Flash Download screen, shown in Figure 5-28, enables the user to download a new image file from a TFTP server to Flash memory.

NOTE

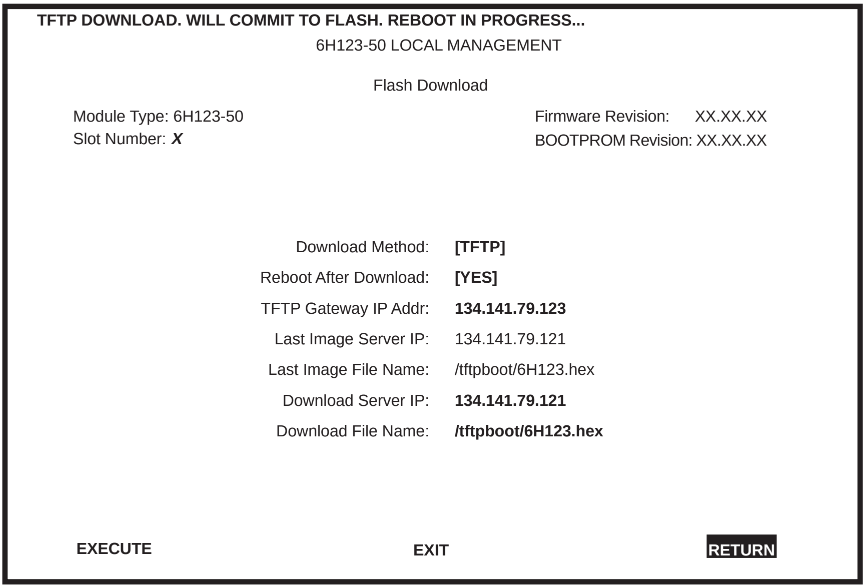
The user may also force a download by changing the position of Switch 6 located inside the module. Refer to Section C.2, for details.

Before downloading a new image to the module, load the image onto the network TFTP server.

NOTE

For information on how to setup a workstation as a TFTP server, refer to the specific workstation documentation.

Access the Flash Download screen from the Module Specific Configuration screen by using the arrow keys to highlight the **FLASH DOWNLOAD** menu item and pressing ENTER. The Flash Download screen displays.



```
TFTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS...
                           6H123-50 LOCAL MANAGEMENT

                               Flash Download

   Module Type: 6H123-50                         Firmware Revision:     XX.XX.XX
   Slot Number: X                                BOOTPROM Revision: XX.XX.XX


                 Download Method:      [TFTP]
           Reboot After Download:      [YES]
           TFTP Gateway IP Addr:       134.141.79.123
            Last Image Server IP:      134.141.79.121
           Last Image File Name:       /tftpboot/6H123.hex
             Download Server IP:       134.141.79.121
             Download File Name:       /tftpboot/6H123.hex


   EXECUTE                         EXIT                               RETURN
```

2276_49

Figure 5-28 Flash Download Screen

NOTE

Download Server IP and Download Server Filename display only when **TFTP** or **RUNTIME** are selected in Download Method.

The following briefly defines each field of the Flash Download screen:

Download Method (Selectable)

This field steps between TFTP, RUNTIME and BOOTP. If set for BOOTP, the module sends out a BootP request to determine the IP address of the TFTP server and the filename of the image to be downloaded. If set for TFTP or RUNTIME, the 6H123-50 and 6H133-37 attempt a TFTP download based on the IP address and filename entered in the fields at the bottom of the Flash Download screen.

Section 5.22.1 describes how to download using TFTP. Section 5.22.2 describes how to download using RUNTIME. Section 5.22.3 describes how to download using BootP.

Reboot After Download (Modifiable when user chooses RUNTIME)
This field notifies the user that the 6H123-50 and 6H133-37 will reboot after the download is complete. If a RUNTIME Download is performed this field toggles between YES and NO. If YES is selected, the module reboots after the download is completed. If NO is selected the module will continue using the existing firmware image. The module stores the new firmware image in FLASH memory. When the module or 6C105 chassis is reset, the module will boot from FLASH memory using the new image.

TFTP Gateway IP Addr (Selectable)
This field shows the IP address of the TFTP gateway server defined in the General Configuration screen in Section 5.15.4, **Setting the TFTP Gateway IP Address**.

Last Image Server IP (Read-only)
This field shows the IP address of the server used for the previous FLASH Download.

Last Image File Name (Read-only)
This field shows the complete path and file name of the last image downloaded to FLASH.

NOTE

If TFTP or RUNTIME is selected as the download method (Figure 5-28), the following two additional fields display.

Download Server IP (Selectable)
The IP address of the TFTP server to be used for the FLASH download is entered in this field.

Download File Name (Selectable)
The complete TFTP server path and file name of the new image is entered in this field.

5.22.1 Image File Download Using TFTP

Set the 6H123-50 and 6H133-37 to download to FLASH using TFTP as follows:

1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to select **TFTP**.
3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
4. Set the IP address of the TFTP gateway server (this defaults to the same IP address as that set in the TFTP Gateway IP Addr field on the General Configuration screen).
5. Use the arrow keys to highlight the **Download Server IP** field.
6. Enter the IP address of the TFTP server using the DDN format.

   For example: 134.141.79.121
7. Use the arrow keys to highlight the **Download File Name** field.
8. Enter the complete path and file name of the image stored on the download server.

   For example: /tftpboot/6H123.hex
9. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message “TFTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS...” displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.22.2 Image File Download Using Runtime

Set the 6H123-50 and 6H133-37 to download to FLASH using RUNTIME as follows:

1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to step to **RUNTIME**.
3. Use the arrow keys to highlight the **Reboot After Download** field.
4. Use the SPACE bar to select either **YES** or **NO**. Select **YES** if you want the module to reboot after the download is complete. Select **NO** if you want the module to store the new image in FLASH memory until the module is manually reset.

5. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.

6. Set the IP address of the TFTP gateway server (this defaults to the same IP address as that set in the TFTP Gateway IP Addr field on the General Configuration screen).

7. Use the arrow keys to highlight the **Download Server IP** field.

8. Enter the IP address of the TFTP server using the DDN format.

   For example: 134.141.79.121

9. Use the arrow keys to highlight the **Download File Name** field.

10. Enter the complete path and file name of the image stored on the download server.

    For example: /tftpboot/6H123.fls

11. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message “RUNTIME DOWNLOAD. WILL COMMIT TO FLASH.” displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.22.3 Image File Download Using BootP

Set the 6H123-50 and 6H133-37 to download to FLASH using BootP as follows:

1. Use the arrow keys to highlight the **Download Method** field.

2. Use the SPACE bar to select **BOOTP**.

3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.

4. Set the IP address of the TFTP gateway server (this defaults to the same IP address set in the TFTP Gateway IP Addr field in the General Configuration screen).

5. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message “BOOTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS...” displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.23 PORT REDIRECT FUNCTION SCREEN

The Port Redirect Function screen, Figure 5-29, enables the user to set each one of the ports on the 6H123-50 and 6H133-37 as a source or destination port. Any port can be set to have one or more destination ports. For example, port 1 can be set as a source port with three destinations, ports 2, 3, and 4. Traffic from port 1 is then automatically redirected to ports 2, 3, and 4. Port 1 can also serve as a destination port for other ports. The port redirect function is extremely useful for troubleshooting purposes, as it allows traffic to be sent to a particular port(s) where, with the use of an analyzer or RMON probe, all current traffic from the source port(s) can be examined. Table 5-5 shows the CONN/port organization.

Table 5-5 CONN/Port Organization

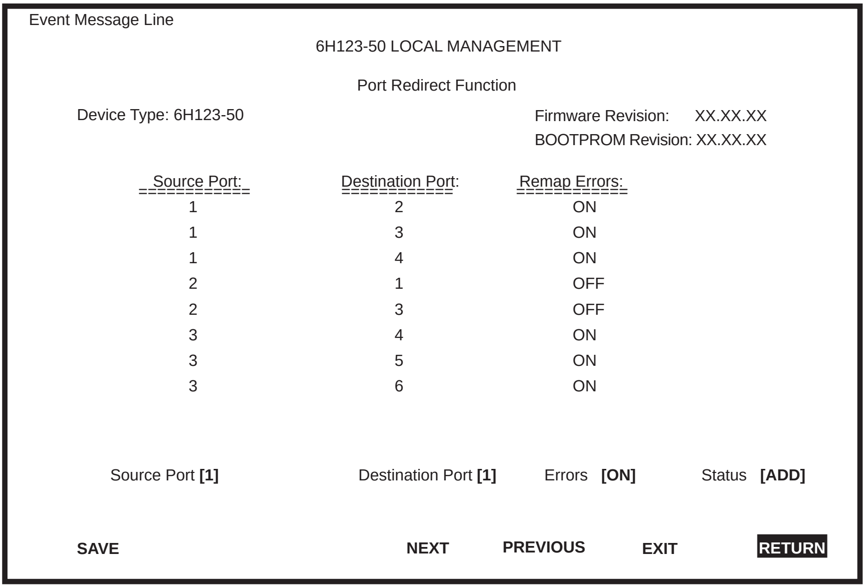
6H123-50	6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 4 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	HSIM = Port 7
Fast Ethernet Slot 5 = Port 9	
Fast Ethernet Slot 6 = Port 10	

NOTE

Although all traffic from the source port (including, if desired, errored frames) is sent to the destination port, normal switching is still performed for all frames on the source port.

Port Redirect operates at a switch interface level and not at a repeater port level. If traffic is redirected to interfaces that include active repeater ports then the redirected traffic is transmitted out all of the repeater ports connected to the interface.

Access the Port Redirect Function screen from the Module Specific Configuration Menu screen by using the arrow keys to highlight the **PORT REDIRECT FUNCTION** menu item and pressing ENTER. The Port Redirect Function screen displays.



```
Event Message Line
                                6H123-50 LOCAL MANAGEMENT

                                  Port Redirect Function
      Device Type: 6H123-50                               Firmware Revision:    XX.XX.XX
                                                          BOOTPROM Revision: XX.XX.XX

           Source Port:           Destination Port:    Remap Errors:
           ============           ============         ============
                1                        2                   ON
                1                        3                   ON
                1                        4                   ON
                2                        1                   OFF
                2                        3                   OFF
                3                        4                   ON
                3                        5                   ON
                3                        6                   ON


        Source Port [1]           Destination Port [1]   Errors   [ON]      Status   [ADD]


      SAVE                              NEXT      PREVIOUS      EXIT          RETURN
```

22861_22

Figure 5-29   Port Redirect Function Screen

The following definitions briefly define each field of the Port Redirect Function screen:

Source Port (Read-only)

Shows which ports are currently set as source ports.

Destination Port (Read-only)

Shows which ports are currently set as destination ports.

Remap Errors (Read-only)

Displays whether the corresponding source ports are configured (ON) to send errored frames to the destination ports, or (OFF) to drop all errored frames and only forward traffic without errored frames to the destination ports.

Source Port [*n*] (Selectable)
Allows a selected port [*n*] to be changed to a source port.

Destination Port [*n*] (Selectable)
Allows a selected port [*n*] to be changed to a destination port.

Errors (Toggle)
User may select ON or OFF to either send errored frames or to drop errored frames and send only valid traffic to the destination port.

Status (Selectable)
Enables you to add or delete the source and destination ports selected in the **Source Port [*n*]** and **Destination Port [*n*]** fields.

5.23.1 Displaying the Source and Destination Entries

There can be more than one Port Redirect Function screen depending on the number of port redirect entries. Each screen displays up to 10 port redirect entries. If there is more than one screen of redirect entries, the NEXT and/or PREVIOUS commands display at the bottom of the screen, allowing the user to navigate to either the next or previous screen.

For example, with three screens of entries, the NEXT command displays at the bottom of the first screen. In the second screen, the NEXT and PREVIOUS commands display. In the last screen, only the PREVIOUS command displays.

To display the next screen, use the arrow keys to highlight NEXT. Press ENTER and the next screen of entries displays.

To display the previous screen, use the arrow keys to highlight PREVIOUS. Press ENTER to view the entries in the previous screen.

5.23.2 Changing Source and Destination Ports

Add or delete source port and destination port entries as follows:

1. Use the arrow keys to highlight the **Source Port** field.
2. Press the SPACE bar or BACKSPACE one or more times to increment or decrement the port number displayed in the brackets [*n*] until the appropriate port number displays.
3. Use the arrow keys to highlight the **Destination Port** field.
4. Use the SPACE bar or BACKSPACE to step to the appropriate port number for the destination port.
5. Use the arrow keys to highlight **ADD** or **DEL** in the Status field.
6. Use the SPACE bar to set Status to either **ADD** or **DEL** (delete) and press ENTER. This adds or deletes the port selections made in steps 2 and 4 and also updates the screen Source Port and Destination Port list.
7. Use the arrow keys to highlight **ON** or **OFF** in the Errors field.
8. Use the SPACE bar to set Errors to either **ON** or **OFF** and press ENTER. **ON** forces the source port to forward errored frames to the destination port(s). **OFF** forces the errored to be dropped before forwarding traffic.

NOTE

If more than one port is to be redirected, repeat steps 1 through 8 for each additional setting, then go to step 9 to save all the new settings at once.

9. Use the arrow keys to highlight **SAVE** at the bottom of the screen. Press ENTER. The message “SAVED OK” displays. This saves the new settings and updates the Source Port and Destination Port read-only fields.

5.24 BROADCAST SUPPRESSION SCREEN

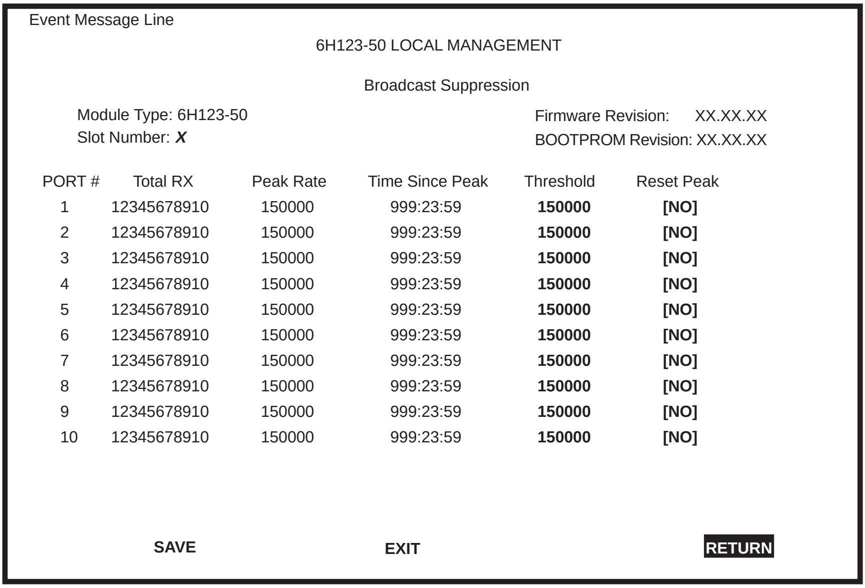
The Broadcast Suppression screen, Figure 5-30, enables the user to set a desired limit of receive broadcast frames per port per second.

NOTES

The Broadcast Suppression screen will not be available if the operational mode of the module has been set to SECURE FAST VLAN. This screen may only be used by modules configured to operate as 802.1D and 802.1Q switches.

Any broadcast frames received above the desired threshold will be dropped.

To access the Broadcast Suppression screen from the Module Specific Configuration screen use the arrow keys to highlight the **BROADCAST SUPPRESSION** menu item and press ENTER. The Broadcast Suppression screen displays.



```
Event Message Line
                              6H123-50 LOCAL MANAGEMENT

                                 Broadcast Suppression

      Module Type: 6H123-50                              Firmware Revision:     XX.XX.XX
      Slot Number: X                                     BOOTPROM Revision: XX.XX.XX

  PORT #     Total RX       Peak Rate     Time Since Peak    Threshold     Reset Peak
    1      12345678910       150000         999:23:59         150000          [NO]
    2      12345678910       150000         999:23:59         150000          [NO]
    3      12345678910       150000         999:23:59         150000          [NO]
    4      12345678910       150000         999:23:59         150000          [NO]
    5      12345678910       150000         999:23:59         150000          [NO]
    6      12345678910       150000         999:23:59         150000          [NO]
    7      12345678910       150000         999:23:59         150000          [NO]
    8      12345678910       150000         999:23:59         150000          [NO]
    9      12345678910       150000         999:23:59         150000          [NO]
    10     12345678910       150000         999:23:59         150000          [NO]


            SAVE                         EXIT                              RETURN
```

2276_56

Figure 5-30 Broadcast Suppression Screen

The following defines each Broadcast Suppression screen field:

PORT # (Read-Only)
Identifies the number of the switched port. Table 5-6 shows the port organization for each module.

Table 5-6 CONN/Port Organization

6H123-50	6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 4 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	HSIM = Port 7
Fast Ethernet Slot 5 = Port 9	
Fast Ethernet Slot 6 = Port 10	

Total RX (Read-Only)
Displays the total number of broadcast frames received.

Peak Rate (Read-Only)
Displays the number of broadcast frames received per second.

Time Since Peak (Read-Only)
Displays the time since peak broadcast frames received.

Threshold (Modifiable)
Enables the user to set the desired limit of receive broadcast frames that will be forwarded per port per second.

Reset Peak (Toggle)
Enables the user to reset the peak rate. Resetting the Peak Rate also resets the Time Since Peak field. The Reset Peak field toggles between YES and NO.

5.24.1 Setting the Threshold

To set the Threshold, proceed as follows:

1. Use the arrow keys to highlight the **Threshold** field for the selected port.
2. Type in the numbers for the desired limit in increments of 10 (for example: 10, 20, 30 etc.)
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

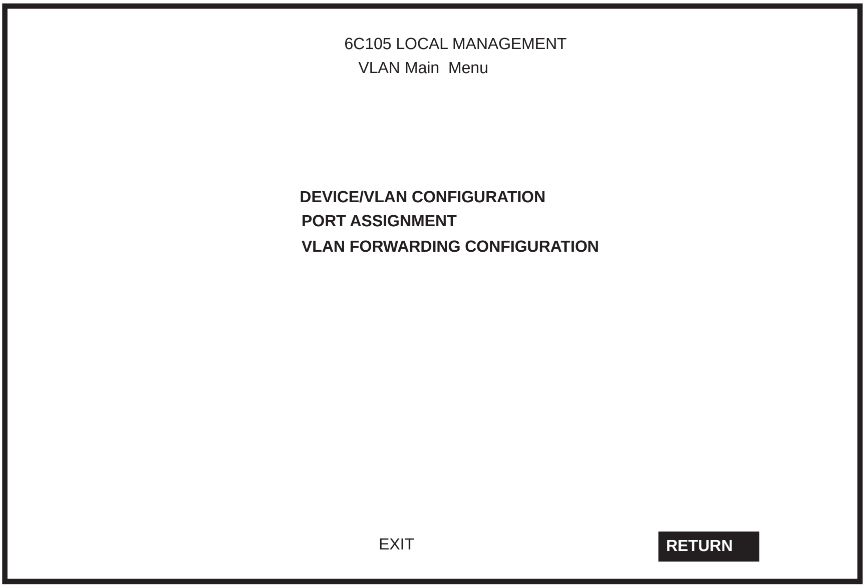
5.24.2 Setting the Reset Peak Switch

To set the Reset Peak Switch field to YES or NO, proceed as follows:

1. Use the arrow keys to highlight the **Reset Peak** field for the selected port.
2. Press the SPACE bar to select **YES** or **NO**.
3. Use the arrows keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.25 VLAN MAIN MENU (802.1Q) SCREEN

The VLAN Main Menu (802.1Q) screen accesses VLAN functionality. Select the **802.1Q VLAN CONFIGURATION** menu item from the Module Specific Configuration Menu and press RETURN. The VLAN Main Menu (802.1Q) screen displays.



6C105 LOCAL MANAGEMENT
VLAN Main Menu

DEVICE/VLAN CONFIGURATION
PORT ASSIGNMENT
VLAN FORWARDING CONFIGURATION

Figure 5-31 VLAN Main Menu Screen

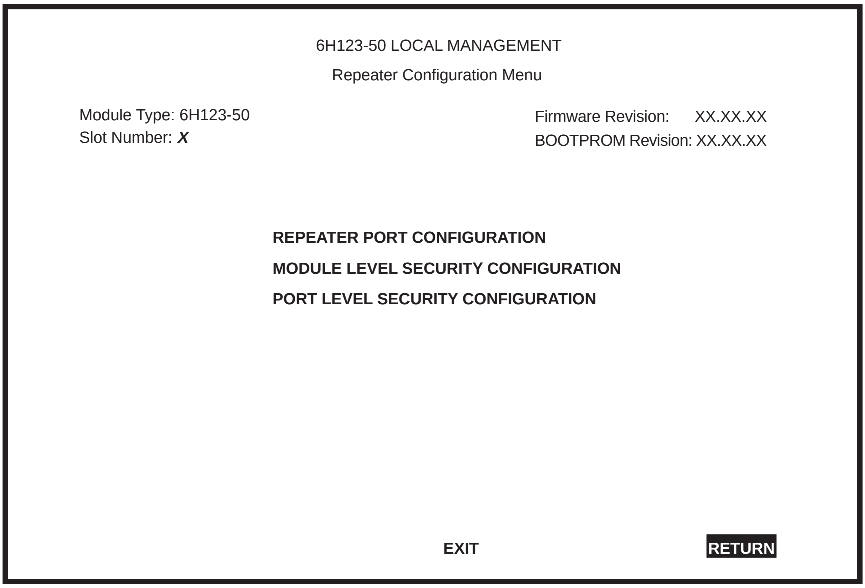
NOTE

The VLAN Main Menu screen is not available if the operational mode of the device is set to either 802.1D SWITCHING or SECURE FAST VLAN. This screen is only used by devices configured to operate as an 802.1Q switch.

Refer to the Cabletron Systems *Port Based VLAN User's Guide* for information on 802.1Q VLAN.

5.26 REPEATER CONFIGURATION MENU SCREEN

The Repeater Configuration Menu screen, Figure 5-32, is used to access the Repeater Port Configuration, Repeater Level Security Configuration, or Port Level Security Configuration screen. To access the Repeater Configuration Menu screen from the Module Specific Configuration Menu screen, select the **REPEATER CONFIGURATION MENU** item and press ENTER. The Repeater Configuration Menu screen displays.



```
                    6H123-50 LOCAL MANAGEMENT
                   Repeater Configuration Menu

Module Type: 6H123-50                      Firmware Revision:   XX.XX.XX
Slot Number: X                             BOOTPROM Revision: XX.XX.XX


                REPEATER PORT CONFIGURATION
                MODULE LEVEL SECURITY CONFIGURATION
                PORT LEVEL SECURITY CONFIGURATION




                          EXIT                          RETURN
```

2745_104

Figure 5-32 Repeater Configuration Menu Screen

The following introduces each screen that is accessible from the Repeater Configuration Menu.

REPEATER PORT CONFIGURATION

Used to monitor the link status and current operating mode of each port on the 10-Mbps or 100-Mbps network of a front panel connector, and also turn each port on or off. For details, refer to Section 5.27.

MODULE LEVEL SECURITY CONFIGURATION

Used to set the state of security for each port of a connector. All ports on a connector can be set to receive all frames (NonSecure state), lock on the source address of the next frame received (LockOnNext), or lock on the address of the last frame received (LockedOnAddr). For details, refer to Section 5.28.

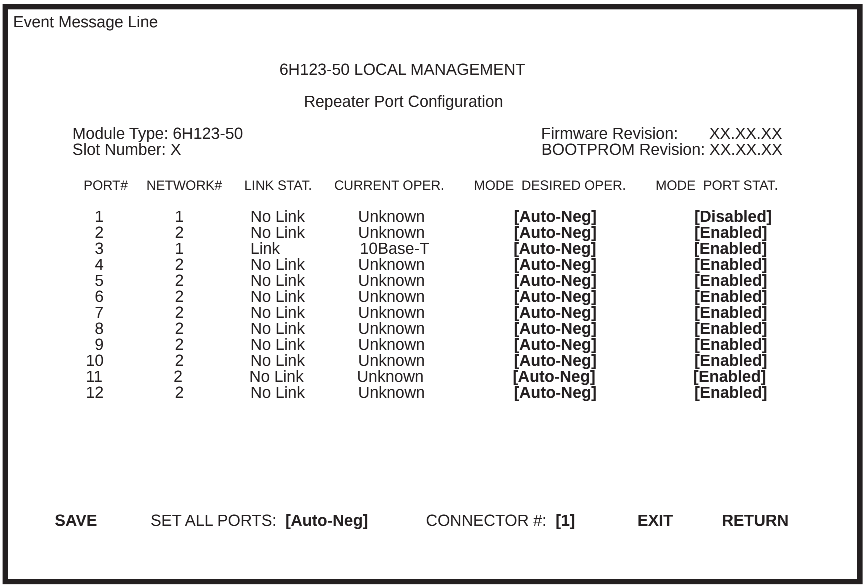
PORT LEVEL SECURITY CONFIGURATION

Used to set the security for all ports of a connector. For details, refer to Section 5.29.

5.27 REPEATER PORT CONFIGURATION SCREEN

The Repeater Port Configuration screen, Figure 5-33, is used to monitor the link status and current operating mode of each port on a 10-Mbps or 100-Mbps network of a front panel connector. The screen is also used to change the operating mode, and turn each port on (enable) or off (disable).

To access the Repeater Port Configuration screen, use the arrow keys to highlight the **REPEATER PORT CONFIGURATION** menu item from the Repeater Configuration Menu screen and press ENTER. The Repeater Port Configuration screen displays.



```
Event Message Line

                              6H123-50 LOCAL MANAGEMENT

                                Repeater Port Configuration

     Module Type: 6H123-50                                     Firmware Revision:      XX.XX.XX
     Slot Number: X                                            BOOTPROM Revision: XX.XX.XX

      PORT#    NETWORK#    LINK STAT.    CURRENT OPER.    MODE  DESIRED OPER.    MODE  PORT STAT.

        1         1         No Link       Unknown              [Auto-Neg]              [Disabled]
        2         2         No Link       Unknown              [Auto-Neg]              [Enabled]
        3         1         Link           10Base-T            [Auto-Neg]              [Enabled]
        4         2         No Link       Unknown              [Auto-Neg]              [Enabled]
        5         2         No Link       Unknown              [Auto-Neg]              [Enabled]
        6         2         No Link       Unknown              [Auto-Neg]              [Enabled]
        7         2         No Link       Unknown              [Auto-Neg]              [Enabled]
        8         2         No Link       Unknown              [Auto-Neg]              [Enabled]
        9         2         No Link       Unknown              [Auto-Neg]              [Enabled]
       10         2         No Link       Unknown              [Auto-Neg]              [Enabled]
       11         2         No Link       Unknown              [Auto-Neg]              [Enabled]
       12         2         No Link       Unknown              [Auto-Neg]              [Enabled]



   SAVE      SET ALL PORTS:  [Auto-Neg]       CONNECTOR #:  [1]       EXIT      RETURN
```

2276_111

Figure 5-33 Repeater Port Configuration Screen

The following are definitions for each field of the Repeater Port Configuration screen:

PORT# (Read-only)
Indicates the repeater port on the connector selected in the CONNECTOR field. Refer to Table 5-7 for the connector (CONN)/repeater port relationship on the device.

Table 5-7 CONN/Repeater Port Relationship

2H23-50R or 6H123-50	2H33-37R or 6H133-37
CONN 1 = Repeater ports 1 – 12	CONN 1 = Repeater ports 1 – 12
CONN 2 = Repeater ports 13 – 24	CONN 2 = Repeater ports 13 – 24
CONN 3 = Repeater ports 25 – 36	CONN 3 = Repeater ports 25 – 36
CONN 4 = Repeater ports 37 – 48	

NETWORK# (Read-only)

Indicates the network on the connector selected in the CONNECTOR field. Table 5-8 shows the association between the CONN and Network Ports on the device.

Table 5-8 CONN/Port Organization

2H23-50R or 6H123-50	2H33-37R or 6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 3 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	HSIM = Port 7

LINK STAT. (Read-only)

Displays the Link status (Link or No Link) of the port.

CURRENT OPER. (Read-only)

Displays the current operating mode of the port.

MODE DESIRED OPER. (Selectable)

This field steps through the following operating mode options: Auto-Neg (Auto Negotiation), 10Base-T, and 100Base-TX.

- When Auto-Neg. is selected, the port Auto-Negotiates with the device to which it is attached to determine its Operating Mode (10 Mbps or 100 Mbps).
- When 10Base-T is selected, the port is forced to operate in standard Ethernet mode (10 Mbps) only.
- When 100Base-TX is selected, the port is forced to operate in Fast Ethernet mode (100 Mbps) only.

To set the port operating mode, refer to Section 5.27.1.

MODE PORT STAT. (Toggle)

Used to enable (turn on) or disable (turn off) the port. To set the port to operating mode, refer to Section 5.27.2.

SET ALL PORTS (Selectable)

Used to select operating mode for all the ports on the connector simultaneously. This field steps through the following selections: Auto-Neg., 10Base T, and 100Base-TX. To set all networks to the same operating mode, refer to Section 5.27.3.

CONNECTOR # (Selectable)

Selects the front panel connector to which the settings will be applied.

5.27.1 Setting the Port Operating Mode

To set the operating mode for one or more network ports, proceed as follows:

1. Use the arrow keys to highlight the **CONNECTOR #** field.
2. Use the SPACE bar to step to the appropriate connector number.
3. Use the arrow keys to highlight the **MODE DESIRED OPER.** field of the network being configured.
4. Use the SPACE bar to step to the appropriate Operating Mode (Auto-Neg, 10Base-T, or 100Base-TX).
5. If setting the operating mode on other ports, repeat steps 3 and 4 for each one and then proceed to step 6.

6. Use the arrow keys to highlight the **SAVE** command.
7. Press ENTER. The message “SAVED OK” displays and all operating mode settings are saved.

5.27.2 Enabling /Disabling Ports

To enable or disable one or more ports, proceed as follows:

1. Use the arrow keys to highlight the **CONNECTOR #** field.
2. Use the SPACE bar to step to the number of the connector containing the network(s) to be enable or disabled.
3. Use the arrow keys to highlight the **MODE PORT STAT.** field of the network being enabled or disabled.
4. Use the SPACE bar to toggle to the appropriate setting (Enabled or Disabled).
5. If setting more than one network, repeat steps 3 and 4 for each one and then proceed to step 6.
6. Use the arrow keys to highlight the **SAVE** command.
7. Press ENTER. The message “SAVED OK” displays and all settings are saved.

5.27.3 Setting All Ports

All the network ports on a connector can be set to the same operating mode simultaneously using the SET ALL PORTS field, as follows:

1. Use the arrow keys to highlight the **CONNECTOR #** field.
2. Use the SPACE bar to step to the appropriate connector number.
3. Use the arrow keys to highlight the **SET ALL PORTS** field.
4. Use the SPACE bar to step to the appropriate Operating Mode (Auto-Neg, 10Base-T, or 100Base-TX).
5. Use the arrow keys to highlight the **SAVE** command.
6. Press ENTER. The message “SAVED OK” displays and all networks of the connector are set to the selected operating mode.

5.27.4 Enabling/Disabling Network Ports

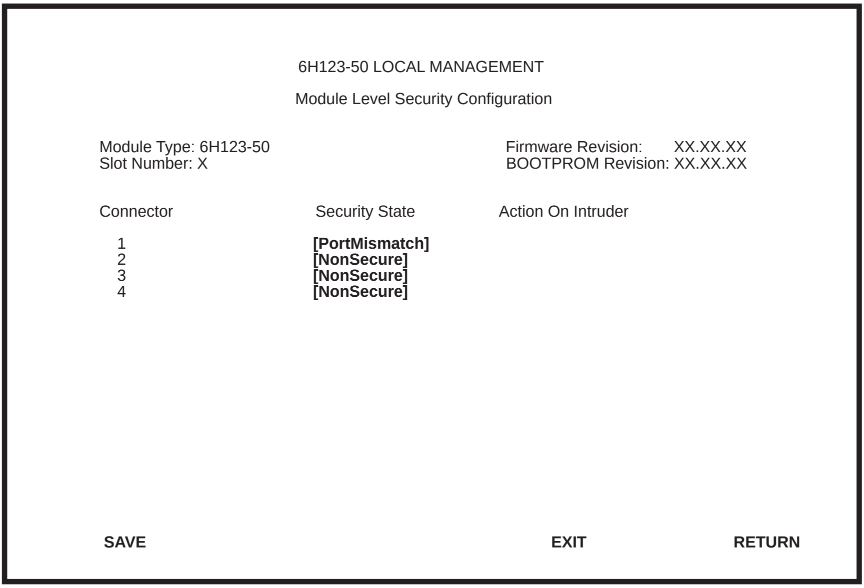
All the network ports on a connector can be set to the same operating mode simultaneously using the SET ALL PORTS field, as follows:

1. Use the arrow keys to highlight the **CONNECTOR #** field.
2. Use the SPACE bar to step to the appropriate connector number.
3. Use the arrow keys to highlight the **SET ALL PORTS** field.
4. Use the SPACE bar to step to the appropriate Operating Mode (Auto-Neg, 10Base-T, or 100Base-TX).
5. Use the arrow keys to highlight the **SAVE** command.
6. Press ENTER. The message “SAVED OK” displays and all networks of the connector are set to the selected operating mode.

5.28 MODULE LEVEL SECURITY CONFIGURATION

The Module Level Security Configuration screen, Figure 5-34, is used to set the state of security according to connector. All ports on a connector can be set to receive all frames (NonSecure state), lock on the source address of the next frame received (LockOnNext) or the source address of the last frame received (LockedOnAddr). When either of the last two options are set, the switch can be set to enable or disable the reception of frames and send or not send traps when an intruder is detected.

To access the Module Level Security Configuration screen, use the arrow keys to highlight the **MODULE LEVEL SECURITY CONFIGURATION** menu item on the Repeater Configuration Menu screen and press ENTER. The Module Level Security Configuration screen displays.



```
                         6H123-50 LOCAL MANAGEMENT

                     Module Level Security Configuration

Module Type: 6H123-50                         Firmware Revision:     XX.XX.XX
Slot Number: X                                BOOTPROM Revision: XX.XX.XX

Connector               Security State           Action On Intruder

  1                     [PortMismatch]
  2                     [NonSecure]
  3                     [NonSecure]
  4                     [NonSecure]









SAVE                                           EXIT              RETURN
```

2276_112

Figure 5-34 Module Level Security Configuration Screen

The following section defines the fields on the Module Level Security Configuration screen.

Connector (Read-Only)

Indicates the connector. Refer to Table 5-9 for the connector (CONN)/repeater port relationship on the device.

Table 5-9 CONN/Repeater Port Relationship

2H23-50R or 6H123-50	2H33-37R or 6H133-37
CONN 1 = Repeater ports 1 – 12	CONN 1 = Repeater ports 1 – 12
CONN 2 = Repeater ports 13 – 24	CONN 2 = Repeater ports 13 – 24
CONN 3 = Repeater ports 25 – 36	CONN 3 = Repeater ports 25 – 36
CONN 4 = Repeater ports 37 – 48	

Security State (Selectable)

Used to select the state of security for frames received by any port on the connector. The states are as follows:

- PortMismatch – Indicates that not all ports on the connector are set to the same state.
- NonSecure – Allows the ports on the connector to receive all frames. The source address of received frames is not examined and the frames are processed in a non secure state.
- LockOnNext – The next frame received by each port is examined to learn its source address. As the source address of a frame is learned on a port, only those frames received with that same source address are processed on that port. As each port is locked on the next address, the device executes the actions selected in the Action On Intruder field
- LockedOnAddr – The source address of the last frame received (or the source address entered in the Port Level Security Configuration screen, if one is entered) is used for security purposes. Once a secure address is defined on a port, only those frames received with that same source address are processed on that port. Any other frame detected with a different address is considered as an intruder, causing the device to execute the actions selected in the Action On Intruder field.

Action On Intruder (Toggle)

Used to select the actions taken for the selected security state. There are two fields to select the actions. Both toggle to activate or deactivate the action.

- DisablePort/NoDisable – DisablePort causes the switch to turn off the port that had a security violation. With NoDisable set, the port is not turned off.
- SendTrap/NoTrap – SendTrap causes the switch to send an SNMP trap when a port detects a security violation. With NoTrap set, no SNMP trap is sent.

5.28.1 Setting the Module Level Security

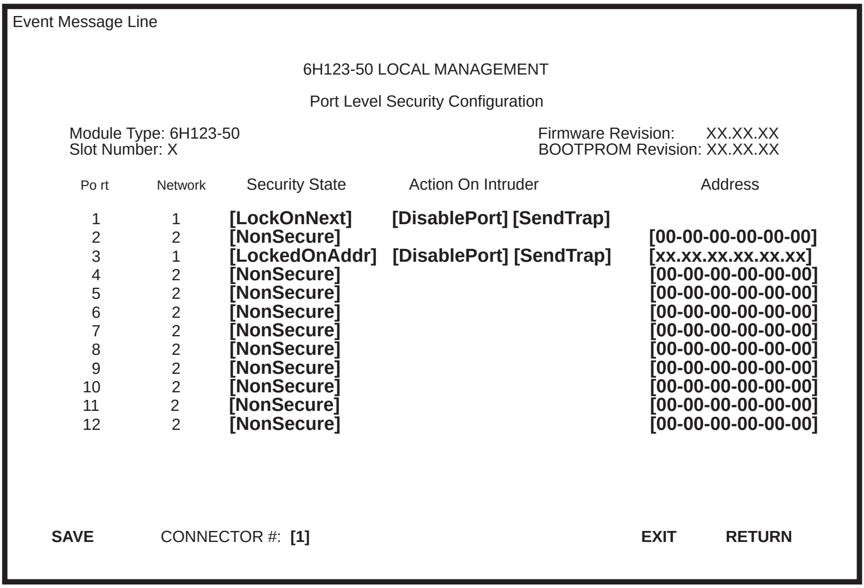
To set module security for each connector, proceed as follows:

1. Use the arrow keys to highlight the **SECURITY STATE** field for the connector.
2. Use the SPACE bar to step to the appropriate security level.
3. If the security level chosen causes the **DisablePort** and **SendTrap** fields to display under Action On Intruder, use the arrow keys to highlight the **DisablePort** field. If the security level chosen does not cause the fields to display under Action On Intruder, proceed to step 7.
4. To change the **DisablePort** setting to **NoDisable**, press the SPACE bar to toggle the setting.
5. Use the arrow keys to highlight the **SendTrap** field.
6. To change the **SendTrap** setting to **NoTrap**, press the SPACE bar to toggle the setting.
7. To change the security on more than one connector, repeat steps 1 through 6 for each connector. Then proceed to step 8 to save all settings at once.
8. Use the arrow keys to highlight the **SAVE** command.
9. Press ENTER. The message “SAVED OK” displays and all ports of the connector are set to the selected operating mode.

5.29 PORT LEVEL SECURITY CONFIGURATION SCREEN

The Port Level Security Configuration screen, Figure 5-35, functions similarly to the Module Level Security Configuration screen, except that it is used to set the security of each port of a selected connector.

To access the Port Level Security Configuration screen, use the arrow keys to highlight the **PORT LEVEL SECURITY CONFIGURATION** menu item on the Repeater Configuration Menu screen and press ENTER. The Port Level Security Configuration screen displays.



```
Event Message Line

                          6H123-50 LOCAL MANAGEMENT

                       Port Level Security Configuration

   Module Type: 6H123-50                          Firmware Revision:     XX.XX.XX
   Slot Number: X                                 BOOTPROM Revision: XX.XX.XX

     Po rt    Network    Security State    Action On Intruder           Address

       1         1      [LockOnNext]     [DisablePort] [SendTrap]
       2         2      [NonSecure]                                 [00-00-00-00-00-00]
       3         1      [LockedOnAddr]   [DisablePort] [SendTrap]   [xx.xx.xx.xx.xx.xx]
       4         2      [NonSecure]                                 [00-00-00-00-00-00]
       5         2      [NonSecure]                                 [00-00-00-00-00-00]
       6         2      [NonSecure]                                 [00-00-00-00-00-00]
       7         2      [NonSecure]                                 [00-00-00-00-00-00]
       8         2      [NonSecure]                                 [00-00-00-00-00-00]
       9         2      [NonSecure]                                 [00-00-00-00-00-00]
      10         2      [NonSecure]                                 [00-00-00-00-00-00]
      11         2      [NonSecure]                                 [00-00-00-00-00-00]
      12         2      [NonSecure]                                 [00-00-00-00-00-00]


   SAVE        CONNECTOR #:  [1]                            EXIT       RETURN
```

2276_113

Figure 5-35 Port Level Security Configuration Screen

The following section defines the fields on the Port Level Security Configuration screen.

Port (Read-only)

Indicates the repeater port on the connector selected in the CONNECTOR # field. Refer to Table 5-10 for the connector/repeater port relationship on the device.

Table 5-10 CONN/Repeater Port Relationship

2H23-50R or 6H123-50	2H33-37R or 6H133-37
CONN 1 = Repeater ports 1 – 12	CONN 1 = Repeater ports 1 – 12
CONN 2 = Repeater ports 13 – 24	CONN 2 = Repeater ports 13 – 24
CONN 3 = Repeater ports 25 – 36	CONN 3 = Repeater ports 25 – 36
CONN 4 = Repeater ports 37 – 48	

Network (Read-only)

Indicates the network to which the port is currently attached. Table 5-11 shows the association between the CONN and Network on the device.

Table 5-11 CONN/Network Organization

2H23-50R or 6H123-50	2H33-37R or 6H133-37
CONN 1 = Network 1, 10 Mbps Network 2, 100 Mbps	CONN 1 = Network 1, 10 Mbps Network 2, 100 Mbps
CONN 2 = Network 3, 10 Mbps Network 4, 100 Mbps	CONN 2 = Network 3, 10 Mbps Network 4, 100 Mbps
CONN 3 = Network 5, 10 Mbps Network 6, 100 Mbps	CONN 3 = Network 5, 10 Mbps Network 6, 100 Mbps
CONN 3 = Network 7, 10 Mbps Network 8, 100 Mbps	HSIM = Port 7

Security State (Selectable)

Used to select the state of security for frames received by a specific port on the connector. The states are as follows:

- PortMismatch – Indicates that not all ports on the connector are set to the same state.
- NonSecure – Allows the ports on the connector to receive all frames. The source address of received frames is not examined and the frames are processed in a non secure state.
- LockOnNext – LockOnNext – The next frame received by each port is examined to learn its source address. As the source address of a frame is learned on a port, only those frames received with that same source address are processed on that port. As each port is locked on the next address, the device executes the actions selected in the Action On Intruder field..
- LockedOnAddr – The source address of the last frame received (or the source address entered in the Port Level Security Configuration screen, if one is entered) is used for security purposes. Once a secure address is defined on a port, only those frames received with that same source address are processed on that port. Any other frame detected with a different address is considered as an intruder, causing the device to execute the actions selected in the Action On Intruder field.

Action On Intruder (Toggle)

Used to select the actions taken for the selected security state. There are two fields to select the actions. Both toggle to activate or deactivate the action.

- DisablePort/NoDisable – DisablePort causes the switch to turn off the port that had a security violation. With NoDisable set, the port is not turned off.
- SendTrap/NoTrap – SendTrap causes the switch to send an SNMP trap when a port detects a security violation. With NoTrap set, no SNMP trap is sent.

Address (Modifiable)
Used to enter the source address for the LockedOnAddr security state setting. Once a secure address is defined on a port, only those frames received with that same source address are processed on that port. Any other frame detected with a different address is considered as an intruder, causing the device to execute the actions selected in the Action On Intruder field. When the security state setting is NonSecure, the field displays the source address of the last frame.

CONNECTOR # (Selectable)
This command field selects the front panel connector (CONN 1 to CONN-3 or CONN 4, depending on the module) to which the port security settings will be applied.

5.29.1 Setting the Port Level Security

To set the security for each repeater port on a connector, proceed as follows:

1. Use the arrow keys to highlight the **CONNECTOR #** field.
2. Use the SPACE bar to step to the appropriate connector number.
3. Use the arrow keys to highlight the **SECURITY STATE** field for a connector.
4. Use the SPACE bar to step to the appropriate security level.
5. If the security level chosen causes the **DisablePort** and **SendTrap** fields to display under Action On Intruder, use the arrow keys to highlight the **DisablePort** field. If the security level chosen does not cause the fields to display under Action On Intruder, proceed to step 9.
6. To change the **DisablePort** setting to **NoDisable**, press the SPACE bar to toggle the setting.
7. Use the arrow keys to highlight the **SendTrap** field.
8. To change the setting to **NoTrap**, press the SPACE bar to toggle the setting.
9. If the security state selected is LockedOnAddr, use the arrow keys to highlight the **Address** field for the port. Otherwise go to step 11.
10. Enter the address to lock on.

11. To change the security on more than one connector, repeat steps 1 through 9 for each connector. Then proceed to step 12 to save all settings at once.

12. Use the arrow keys to highlight the **SAVE** command.

13. Press ENTER. The message “SAVED OK” displays and all ports of the connector are set to the selected operating mode.

5.30 MODULE STATISTICS MENU SCREEN

The Module Statistics Menu screen, Figure 5-36, provides access to screens that enable the user to obtain statistics about traffic through each switch interface and repeater port.

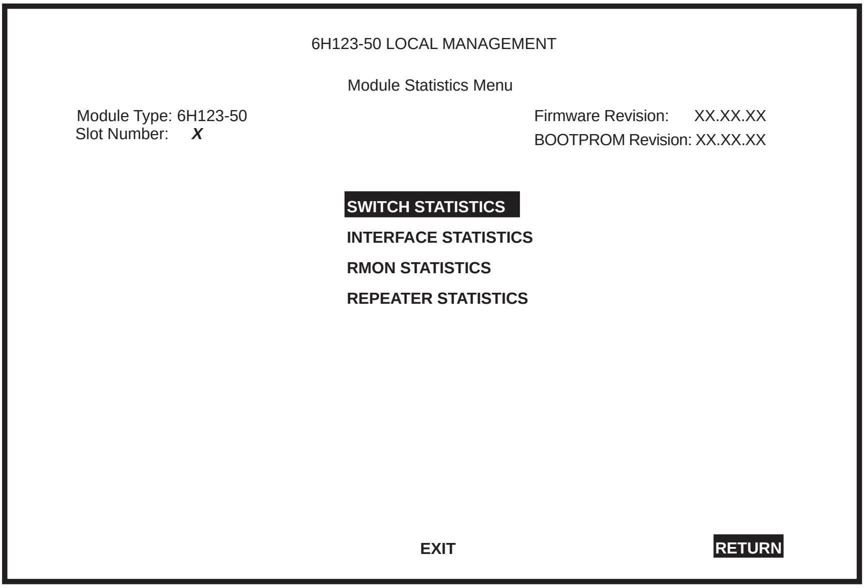
NOTE

The following menu item on the Module Statistics Menu screen will not display if the operational mode of the module has been set to SECURE FAST VLAN:

SWITCH STATISTICS

Section 5.15.9 provides instructions on setting the operational mode.

Access the Module Statistics Menu screen from the Module Menu screen by using the arrow keys to highlight the **MODULE STATISTICS** menu item and pressing ENTER. The Module Statistics Menu screen displays.



6H123-50 LOCAL MANAGEMENT

Module Statistics Menu

Module Type: 6H123-50
Slot Number: *X*

Firmware Revision: XX.XX.XX
BOOTPROM Revision: XX.XX.XX

22511-67

Figure 5-36 Module Statistics Menu Screen

The Module Statistics Menu screen displays the following menu item:

SWITCH STATISTICS

The Switch Statistics screen lists the number of frames received, transmitted, filtered, and forwarded by each interface. For details, refer to Section 5.31.

INTERFACE STATISTICS

The Interface Statistics screen provides the MIB-II statistics for each switched interface, on an interface-by-interface basis. For details, refer to Section 5.32.

RMON STATISTICS

The RMON Statistics screen displays all the statistics gathered by the embedded RMON agent built-in to the 6H123-50 and 6H133-37. For details, refer to Section 5.33.

REPEATER STATISTICS

The Repeater Statistics screen provides the operating statistics for each port and its corresponding network (Network 1–8 for the 6H123-50 and Network 1–6 for the 6H133-37). This screen also displays the statistics for each repeater port.For details, refer to Section 5.34.

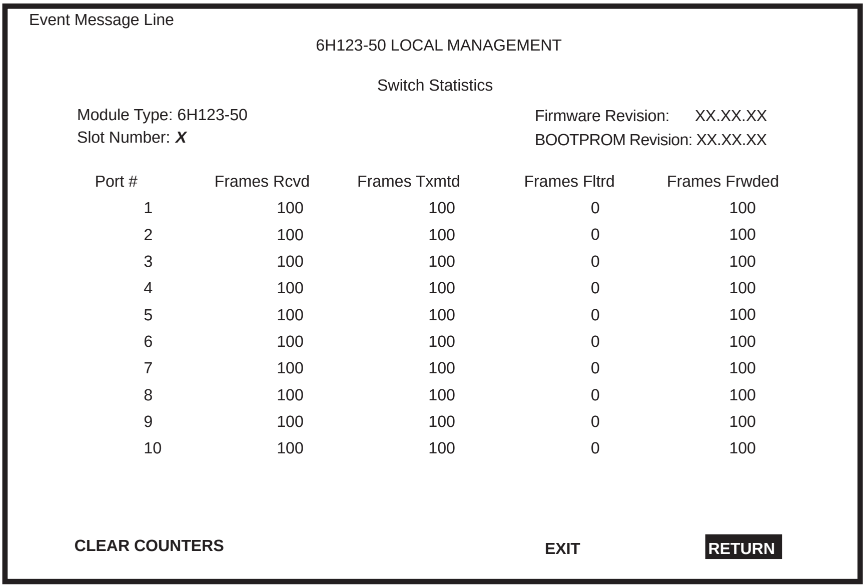
5.31 SWITCH STATISTICS SCREEN

The Switch Statistics screen, Figure 5-37, lists the number of frames received, transmitted, filtered, and forwarded by each interface, including backplane interfaces.

NOTE

The Switch Statistics screen will not be available if the operational mode of the module has been set to SECURE FAST VLAN. This screen may only be used by modules configured to operate as 802.1D or 802.1Q switches.

Access the Switch Statistics screen from the Module Statistics Menu screen by using the arrow keys to highlight the **SWITCH STATISTICS** menu item and pressing ENTER. The Switch Statistics screen displays.



```
Event Message Line
                          6H123-50 LOCAL MANAGEMENT

                              Switch Statistics

    Module Type: 6H123-50                            Firmware Revision:     XX.XX.XX
    Slot Number: X                                   BOOTPROM Revision: XX.XX.XX

      Port #          Frames Rcvd      Frames Txmtd       Frames Fltrd      Frames Frwded
         1                100              100                0                100
         2                100              100                0                100
         3                100              100                0                100
         4                100              100                0                100
         5                100              100                0                100
         6                100              100                0                100
         7                100              100                0                100
         8                100              100                0                100
         9                100              100                0                100
         10               100              100                0                100



    CLEAR COUNTERS                                      EXIT             RETURN
```

22761_26

Figure 5-37 Switch Statistics Screen

The Switch Statistics screen displays the following fields:

Port # (Read-Only)

Identifies the port. There can be ten or seven ports depending on if the device is a 6H123-50 or 6H133-37, respectively. Table 5-12 shows the port organization.

Table 5-12 CONN/Port Organization

6H123-50	6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 4 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	HSIM = Port 7
Fast Ethernet Port 5 = Port 9	
Fast Ethernet Port 6 = Port 10	

Frames Rcvd (Read-Only)

Displays the number of frames received by the interface.

Frames Txmtd (Read-Only)

Displays the number of frames transmitted by the interface.

Frames Fltrd (Read-Only)

Displays the number of frames filtered by the interface.

Frames Frwded (Read-Only)

Displays the number of frames forwarded by the interface.

CLEAR COUNTERS (Command)

This command clears all the counters of the displayed ports to zero. To clear the counters, use the arrow keys to highlight **CLEAR COUNTERS** at the bottom of the screen, then press ENTER.

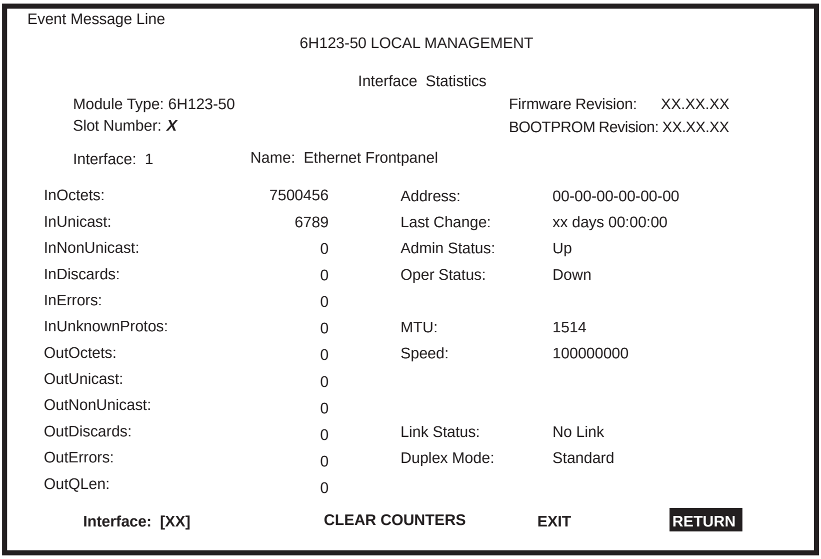
5.32 INTERFACE STATISTICS SCREEN

The Interface Statistics screen is used to gather MIB-II statistics for all of the 6H123-50 and 6H133-37 interfaces (Fast Ethernet Interface Modules and all backplane interfaces) with the exception of an HSIM installed in the 6H133-37.

NOTE

Cabletron Systems HSIMs gather their own statistics, and may be viewed via the Local Management screens of the applicable HSIM. Refer to your HSIM documentation for information on accessing these screens.

Access the Interface Statistics screen by using the arrow keys to highlight the **INTERFACE STATISTICS** menu item on the Module Statistics Menu screen and pressing ENTER. The Interface Statistics screen, Figure 5-38, displays.



```
Event Message Line
                              6H123-50 LOCAL MANAGEMENT

                                   Interface  Statistics
      Module Type: 6H123-50                               Firmware Revision:     XX.XX.XX
      Slot Number: X                                      BOOTPROM Revision: XX.XX.XX

      Interface:  1              Name:  Ethernet Frontpanel

   InOctets:                 7500456      Address:            00-00-00-00-00-00
   InUnicast:                   6789      Last Change:        xx days 00:00:00
   InNonUnicast:                   0      Admin Status:       Up
   InDiscards:                     0      Oper Status:        Down
   InErrors:                       0
   InUnknownProtos:                0      MTU:                1514
   OutOctets:                      0      Speed:              100000000
   OutUnicast:                     0
   OutNonUnicast:                  0
   OutDiscards:                    0      Link Status:        No Link
   OutErrors:                      0      Duplex Mode:        Standard
   OutQLen:                        0

       Interface:  [XX]            CLEAR COUNTERS         EXIT            RETURN
```

2269_64

Figure 5-38 Interface Statistics Screen

The following definitions are for each field of the Interface Statistics screen:

Interface (Read-only)
This field displays the Interface number for which statistics are currently being displayed. Figure 5-38 shows the Interface field displaying 1. This represents port 1 of the module. To view other interface statistics refer to Section 5.32.1.

Name (Read-only)
The Name field displays the type of interface for which statistics are being displayed.

InOctets (Read-only)
This field displays the total number of octets (bytes) that have been received on the Interface. This includes all octets from bad frames and framing characters.

InUnicast (Read-only)
The InUnicast field displays the total number of frames that have been received that were sent to a single address.

InNonUnicast (Read-only)
This field displays the total number of frames that have been received that were delivered to a broadcast or multicast address.

InDiscards (Read-only)
The InDiscards field displays the total number of inbound frames that were discarded, even though the frames contained no errors. This field may increment because the switch needed to free up buffer space, or the switch was overutilized.

InErrors (Read-only)
This field displays the total number of inbound frames that have been discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.

InUnknownProtos (Read-only)
The InUnknownProtos field displays the total number of frames that were discarded because the frames were in an unknown, or unsupported, format.

OutOctets (Read-only)
This field displays the total number of octets (bytes) that have been transmitted from the Interface.

OutUnicast (Read-only)
The OutUnicast field displays the total number of frames transmitted that were sent to a single address.

OutNonUnicast (Read-only)
This field displays the total number of frames transmitted to a broadcast or multicast address.

OutDiscards (Read-only)
The OutDiscards field displays the total number of outbound frames that were discarded, even though the frames contained no errors. This field may increment because the switch needed to free up buffer space or the switch was overutilized.

OutErrors (Read-only)
This field displays the total number of outbound frames discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.

OutQLen (Read-only)
The OutQLen field displays the length of the packet queue. The field represents the total number of packets that can be contained in the queue.

Address (Read-only)
This field displays the MAC Address of the interface that is currently being displayed.

Last Change (Read-only)
This field displays the last time that the interface was reset.

Admin Status (Read-only)
This field displays the current status of the interface. If this field displays “Testing”, no packets will be transmitted or received on this interface.

Oper Status (Read-only)
This field displays the current status of the interface. If this field displays “Testing”, no packets will be transmitted or received on this interface.

MTU (Read-only)
The MTU field displays the maximum frame size (in octets) that a frame may contain to be received or transmitted from this interface.

Speed (Read-only)
The Speed field displays an estimate of the interface’s current bandwidth in bits per second.

Link Status (Read-only)
This field displays the current link status of the interface. This field reads either “Link” or “No Link”.

Duplex Mode (Read-only)
This field indicates whether the interface is operating in normal or full duplex mode. This field reads either “Standard” or “Full Duplex”.

Interface [XX] (Command)
This command is used to enter an interface number for viewing statistics. For instructions on how to use this command refer to Section 5.32.1.

CLEAR COUNTERS (Command)
This command is used to reset all statistic counters to zero. For details on how to use this field, refer to Section 5.32.2.

5.32.1 Displaying Interface Statistics

To display the statistics for any interface, proceed as follows:

1. Use the arrow keys to highlight the **Interface [XX]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL [delete] key to decrement) the interface number.
3. Press ENTER (neither the Interface # fields nor the statistics change until ENTER is pressed).

5.32.2 Using the Clear Counters Command

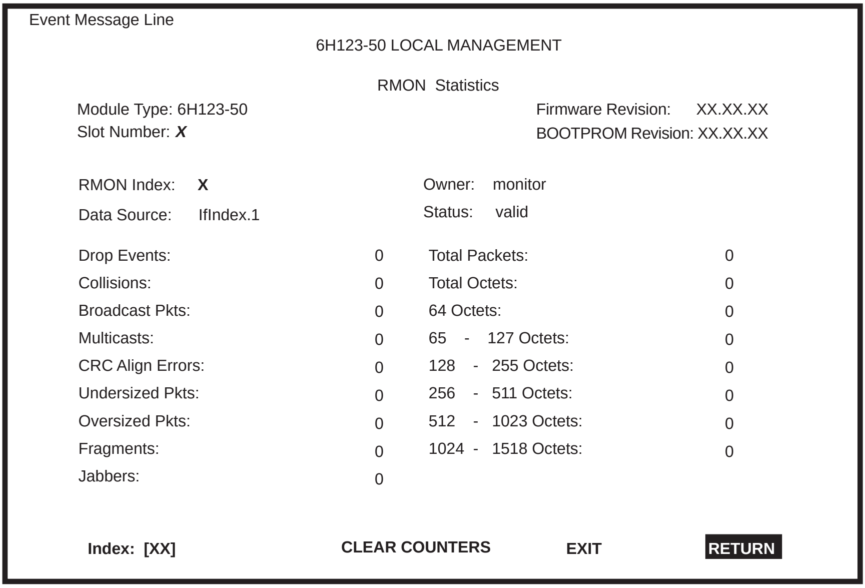
To reset all the statistics counters of the selected interface to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** command field.
2. Press ENTER, the counters for the selected interface are reset to zero.

5.33 RMON STATISTICS SCREEN

RMON statistics for each interface, on a interface-by-interface basis, are viewed through the RMON Statistics screen shown in Figure 5-39.

Access the RMON Statistics screen by using the arrow keys to highlight the **RMON STATISTICS** menu item on the Module Statistics Menu screen and pressing ENTER. The RMON Statistics screen displays.



```
Event Message Line
                            6H123-50 LOCAL MANAGEMENT

                                 RMON  Statistics
   Module Type: 6H123-50                          Firmware Revision:     XX.XX.XX
   Slot Number: X                                 BOOTPROM Revision: XX.XX.XX

   RMON Index:     X                    Owner:     monitor
   Data Source:    IfIndex.1            Status:     valid

   Drop Events:                  0       Total Packets:                 0
   Collisions:                   0       Total Octets:                  0
   Broadcast Pkts:               0       64 Octets:                     0
   Multicasts:                   0       65    -   127 Octets:          0
   CRC Align Errors:             0       128   -   255 Octets:          0
   Undersized Pkts:              0       256   -   511 Octets:          0
   Oversized Pkts:               0       512   -   1023 Octets:         0
   Fragments:                    0       1024  -   1518 Octets:         0
   Jabbers:                      0

    Index:  [XX]           CLEAR COUNTERS          EXIT            RETURN
```

2269_65

Figure 5-39 RMON Statistics Screen

The following definitions explain each field of the RMON Statistics screen:

RMON Index (Read-only)

This field displays the current interface for which statistics are being shown. The 6H123-50 and 6H133-37 have an embedded RMON agent that gathers statistics for each interface on the module.

Data Source (Read-only)

This field displays the source of the statistics data that is currently being displayed on the screen. Figure 5-39 shows that the data source for this RMON index is Interface 1 (Network Port 1, 10 Mbps of CONN 1) by displaying the name IfIndex.1. If the screen displays RMON statistics for Interface 4 (Network Port 4, 100 Mbps bus of CONN 2), the name displayed would be IfIndex.4. Table 5-13 shows the association between the CONN and Network Ports for the 6H123-50 and 6H133-37.

Table 5-13 CONN/Network Interfaces

6H123-50	6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 4 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	

Owner (Read-only)

This field displays the name of the entity that configured this entry.

Status (Read-only)

The Status field displays the current operating status of the displayed interface. This field displays “Valid” or “Invalid”.

Drop Events (Read-only)

This field displays the total number of times that the RMON agent was forced to discard packets due to the lack of available switch resources.

NOTE

The Drop Events field does not display the number of packets dropped, it only displays the number of times that the RMON agent was forced to discard packets. Drop events are a normal occurrence during switch initialization.

Collisions (Read-only)

This field displays the total number of collisions that have occurred on this interface.

Broadcast Pkts (Read-only)

The Broadcast Pkts field displays the total number of good frames that were directed to the broadcast address. The value of this field does not include multicast frames.

Multicasts (Read-only)

The Multicast Pkts field displays the total number of good frames received that were directed to a multicast address. The value of this field does not include frames directed to the broadcast address.

CRC Align Errors (Read-only)

This field displays the number of frames with bad Cyclic Redundancy Checks (CRC) received from the network. The CRC is a 4-byte field in the data frame that ensures that the data received is the same as the data that was originally sent.

Undersized Pkts (Read-only)

The Undersized Packets field displays the number of frames received whose size was less than the minimum Ethernet frame size of 64 bytes, not including preamble, but having a valid CRC.

Oversized Pkts (Read-only)

The Oversized Packets field displays the number of frames received whose size exceeded 1518 data bytes, not including preamble, but having a valid CRC.

Fragments (Read-only)

This field displays the number of received frames that are not the minimum number of bytes in length or received frames that had a bad Frame Check Sequence (FCS), were less than 64 bytes in length (excluding framing bits, but including FCS bytes), and having an invalid FCS (CRC) or classified as an alignment error.

NOTE

It is normal for the Fragments field to increment. This is because the RMON agent increments the field when undersized frames are detected (which are normal occurrences due to collisions) and when noise hits occur.

Jabbers (Read-only)

This field displays the total number of frames that were greater than 1518 bytes and had a bad FCS (CRC).

Total Packets (Read-only)

This field displays the total number of frames (including bad frames, broadcast frames, and multicast frames) received on this interface.

Total Octets (Read-only)

This field displays the total number of octets (bytes) of data, including those in bad frames, received on this interface.

64 Octets (Read-only)

Displays the total number of frames including bad frames, received that were 64 bytes in length (excluding framing bits, but including FCS bytes).

65 - 127 Octets (Read-only)

Displays the total number of frames, including bad frames, received that were between 65 and 127 bytes in length (excluding framing bits, but including FCS bytes).

128 - 255 Octets (Read-only)

Displays the total number of frames, including bad frames, received that were between 128 and 255 bytes in length (excluding framing bits, but including FCS bytes).

256 - 511 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 256 and 511 bytes in length (excluding framing bits, but including FCS bytes).

512 - 1023 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 512 and 1023 bytes in length (excluding framing bits, but including FCS bytes).

1024 - 1518 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 1024 and 1518 bytes in length (excluding framing bits, but including FCS bytes).

Index [XX] (Command)
This command is used to enter an index number for viewing statistics. For instructions on how to use this command refer to Section 5.33.1.

CLEAR COUNTERS (Command)
This command is used to reset all statistic counters to zero. For details on how to use this command, refer to Section 5.33.2.

5.33.1 Displaying RMON Statistics

To display the statistics for any index, proceed as follows:

1. Use the arrow keys to highlight the **Index [XX]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL [delete] key to decrement) the index number.
3. Press ENTER (neither the **RMON Index #** field nor the statistics change until ENTER is pressed).

5.33.2 Using the Clear Counters Command

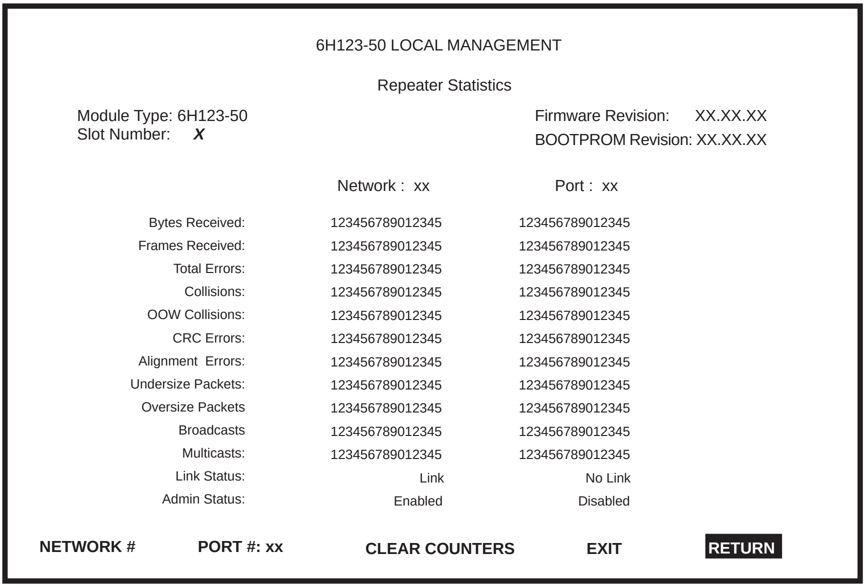
To reset all the statistics counters of the selected interface to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** command.
2. Press ENTER, the counters for the selected index are reset to zero.

5.34 REPEATER STATISTICS SCREEN

Operating statistics for each repeater port and its corresponding network (CONNs 1–4 and CONNs 1–3) are displayed via the Repeater Statistics screen shown in Figure 5-40.

To access the Repeater Statistics screen, use the arrow keys to highlight the **REPEATER STATISTICS** menu item on the Module Statistics Menu screen and press ENTER. The Repeater Statistics screen displays.



```
                         6H123-50 LOCAL MANAGEMENT

                            Repeater Statistics

    Module Type: 6H123-50                      Firmware Revision:     XX.XX.XX
    Slot Number:    X                          BOOTPROM Revision: XX.XX.XX

                            Network :  xx           Port :  xx

           Bytes Received:    123456789012345    123456789012345
          Frames Received:    123456789012345    123456789012345
             Total Errors:    123456789012345    123456789012345
               Collisions:    123456789012345    123456789012345
           OOW Collisions:    123456789012345    123456789012345
               CRC Errors:    123456789012345    123456789012345
         Alignment  Errors:   123456789012345    123456789012345
        Undersize Packets:    123456789012345    123456789012345
          Oversize Packets    123456789012345    123456789012345
               Broadcasts     123456789012345    123456789012345
               Multicasts:    123456789012345    123456789012345
              Link Status:               Link            No Link
             Admin Status:            Enabled           Disabled

  NETWORK #       PORT #: xx       CLEAR COUNTERS       EXIT       RETURN
```

22511-29

Figure 5-40 Repeater Statistics Screen

The following definitions explain each field of the Repeater Statistics screen:

Network (Read-Only)

Indicates the current network port (1 through 8, 6H123-50 or 1 through 6, 6H133-37) for which statistics are displayed. This field is automatically set by selecting a port number in the PORT # command field at the bottom of the screen. For example, if 4 is selected in the PORT # command field, the statistics for Network 4 (CONN 2, 100 Mbps Network Port) displays along with the statistics for the selected port.

Table 5-14 shows the association between the CONN and Network Ports for the 6H123-50 and 6H133-37.

Table 5-14 CONN/Port Organization

6H123-50	6H133-37
CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps	CONN 1 = Network Port 1, 10 Mbps Network Port 2, 100 Mbps
CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps	CONN 2 = Network Port 3, 10 Mbps Network Port 4, 100 Mbps
CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps	CONN 3 = Network Port 5, 10 Mbps Network Port 6, 100 Mbps
CONN 3 = Network Port 7, 10 Mbps Network Port 8, 100 Mbps	HSIM = Port 7

Port (Read-Only)

Indicates the current repeater port for which statistics are displayed. The port number can be changed by using the PORT # command field at the bottom of the screen. Depending on the port number entered, the Network # field will automatically change to indicate the associated Network Port. Table 5-15 shows CONN/repeater port relationship.

Table 5-15 CONN/Repeater Port Relationship

6H123-50	6H133-37
CONN 1 = Repeater ports 1 – 12	CONN 1 = Repeater ports 1 – 12
CONN 2 = Repeater ports 13 – 24	CONN 2 = Repeater ports 13 – 24
CONN 3 = Repeater ports 25 – 36	CONN 3 = Repeater ports 25 – 36
CONN 4 = Repeater ports 37 – 48	

Bytes Received (Read-only)

Displays the number of bytes received.

Frames Received (Read-only)

Displays the number of frames received.

Total Errors (Read-only)
Displays the total number of errors.

Collisions (Read-only)
Displays the total number of collisions that were detected.

OOW Collisions (Read-only)
Displays the number of Out Of Window (OOW) collision errors detected. These collisions can be caused by a station on the network violating Carrier Sense and transmitting at will, a cable failure occurring during the transmission of a packet, or a network propagation delay greater than 51.2 µs.

CRC Errors (Read-only)
Displays the number of packets with bad Cyclic Redundancy Checks (CRC) received from the network. The CRC is a 4-byte field in the data packet that ensures that the data that is received is the same as the data that was originally sent.

Alignment Errors (Read-only)
Displays the number of alignment errors detected. Alignment errors occur when the total number of bits in a frame are not divisible by eight due to missing bits in the bytes contained in the frame.

Undersize Packets (Read-only)
Displays the number of packets received with a valid CRC and whose size was less than the minimum Ethernet frame size of 64 bytes (not including the preamble).

Oversize Packets (Read-only)
Displays the number of packets received with a valid CRC and whose size exceeded 1518 data bytes (not including preamble).

Broadcasts (Read-only)
Displays the number of broadcasts transmitted and received.

Multicasts (Read-only)
Displays the number of multicasts transmitted and received.

Link Status (Read-only)
Indicates if the network or port is linked (**Link**) or not linked (**No Link**).

Admin Status (Read-only)
Indicates if the network or port is enabled (**Enabled**) or disabled (**Disabled**).

NETWORK # (Command)
This command is used to select a particular Network to view its statistics. When the Network is selected the statistics are also displayed for the first port in the Network under Port #. For details, refer to Section 5.34.1.

PORT # (Command)
This command is used to select a port to view its statistics and those of its associated Network. For details, refer to Section 5.34.2.

CLEAR COUNTERS (Command)
This command sets all statistics counters to zero. For details on how to use this command, refer to Section 5.34.3.

5.34.1 Displaying Network Statistics

To display the statistics of any Network, proceed as follows:

1. Use the arrow keys to highlight the **NETWORK #** command field at the bottom of the screen.
2. Press the SPACE bar to increment or press the BACKSPACE key to decrement the port number.
3. Press ENTER (the NETWORK #, the first PORT # of the Network, and the associated statistics do not display until ENTER is pressed).

5.34.2 Displaying Repeater Statistics

To display the statistics for any port, proceed as follows:

1. Use the arrow keys to highlight the **PORT #** command field at the bottom of the screen.
2. Press the SPACE bar to increment or press the BACKSPACE key to decrement the port number.
3. Press ENTER (the PORT #, the NETWORK #, and the statistics do not change until ENTER is pressed).

5.34.3 Using the Clear Counters Command

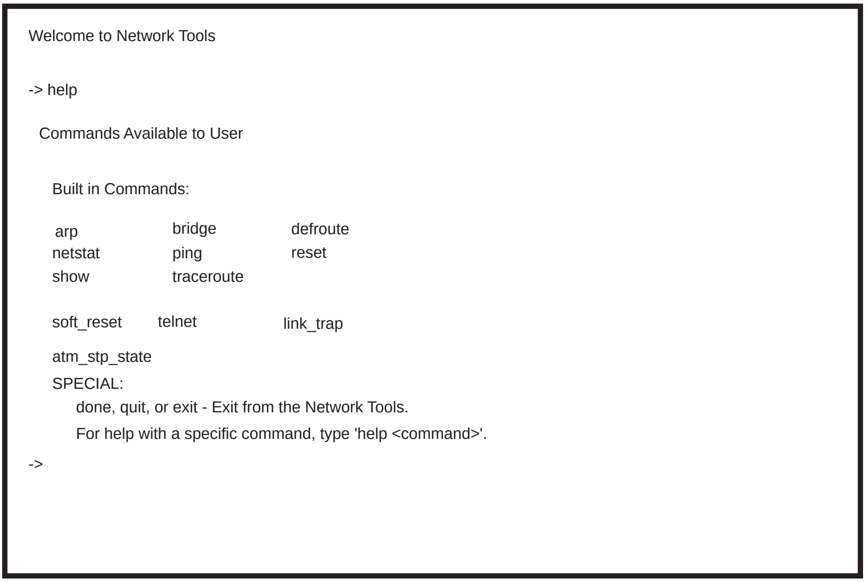
To reset all the statistics counters of the selected port to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** command field at the bottom of the screen.
2. Press ENTER, the counters for the selected port are reset to zero.

5.35 NETWORK TOOLS

The Network Tools function enables the user to access and manage network devices. Figure 5-41 shows the Network Tools help screen.

To access the Network Tools screen, use the arrow keys to highlight the **NETWORK TOOLS** menu item in the Device Menu screen and press ENTER. The Network Tools screen displays.



```
Welcome to Network Tools

-> help

  Commands Available to User

    Built in Commands:

     arp              bridge          defroute
    netstat           ping            reset
    show              traceroute

    soft_reset     telnet            link_trap

    atm_stp_state
    SPECIAL:
        done, quit, or exit - Exit from the Network Tools.
        For help with a specific command, type 'help <command>'.
->
```

090829

Figure 5-41 Network Tools Screen

The Network Tools functions are performed using a series of commands. Entering commands in Network Tools involves typing the command to be executed at the Network Tools prompt, adding any desired or required extensions, and pressing ENTER.

There are two categories of commands in the command set.

- Built-in Commands **–** Allow the user to access and manage network devices. The commands are: **arp**, **bridge**, **defroute**, **netstat**, **ping**, **reset**, **show**, **traceroute**, **soft-reset**, **telnet, link_trap,** and **atm_stp_state**.
- Special Commands **–** Allow the user to exit from Network Tools. The commands are **done**, **exit**, and **quit**.

NOTE

The conventions used in describing the commands in Network Tools are as follows:

Arguments enclosed by [ ] are required.

Arguments enclosed by < > are optional.

In the following command examples, the information entered by user is shown in **bold** Helvetica font.

To abort the output or interrupt a process, press the CONTROL key and c key simultaneously, designated as ^C here.

The commands are presented in the following format:

command:

Syntax: Shows the required command format. It indicates where arguments, if any, must be specified.

Description: Briefly describes the command and its uses.

Options: Lists any additional fields in the appropriate format which may be added to the command.

Example: Shows an example of the command.

5.35.1 Built-in Commands

The built-in commands listed in this section activate functions on the LM managed device or devices being accessed through Network Tools.

arp:

Syntax: arp <options>

Description: The arp command provides access to the ARP (Address Resolution Protocol) cache, enabling you to view cache data, delete entries, or add a static route. Super-user access is required to delete an entry or add a static route.

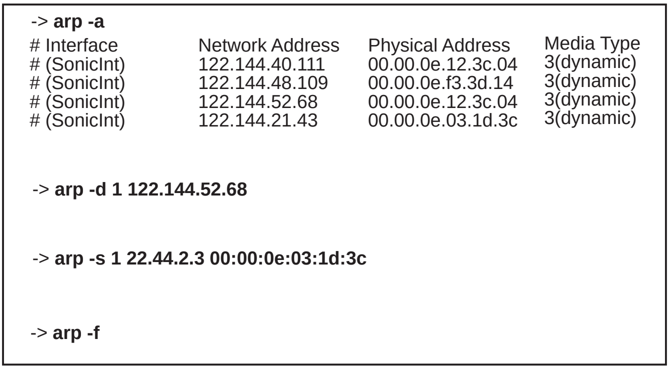
Each ARP cache entry lists the network *interface* that the device is connected to, the device’s *network address* or IP address, the device’s *physical address* or MAC address, and the *media type* of connection to the device. Media types display as numbers, which stand for the following states:

1 - Other
2 - Invalid entry (cannot ping device, timed out, etc.)
3 - Dynamic route entry
4 - Static route entry (not subject to change)

You can specify the arp command without options, or with one of the following options:

Options: -a Views cache data
-d Deletes an IP address entry. Requires additional arguments: <Interface Number> <IP address>
-s Adds a static entry. Requires additional arguments: <Interface Number> <IP address> <MAC address>
-f Flushes the ARP cache

Example:



```
-> arp -a
# Interface          Network Address     Physical Address     Media Type
# (SonicInt)         122.144.40.111      00.00.0e.12.3c.04    3(dynamic)
# (SonicInt)         122.144.48.109      00.00.0e.f3.3d.14    3(dynamic)
# (SonicInt)         122.144.52.68       00.00.0e.12.3c.04    3(dynamic)
# (SonicInt)         122.144.21.43       00.00.0e.03.1d.3c    3(dynamic)


-> arp -d 1 122.144.52.68


-> arp -s 1 22.44.2.3 00:00:0e:03:1d:3c


-> arp -f
```

05141-67

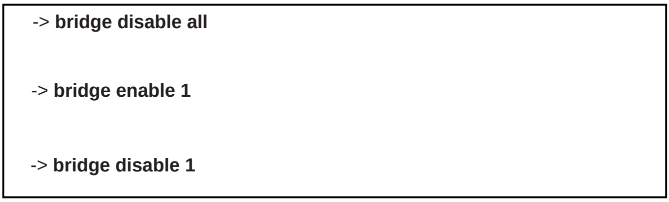
bridge:

Syntax: bridge [ENABLE/DISABLE] [IFNUM/ALL]

Description: The bridge command allows bridge management to be enabled or disabled at the user’s request, either one at a time or all at once. Specifying a single interface number will affect the bridging status of that interface, while specifying ALL will affect every interface.

Options: Not Applicable

Example:



```
-> bridge disable all


-> bridge enable 1


-> bridge disable 1
```

05141-68

defroute:

Syntax: defroute

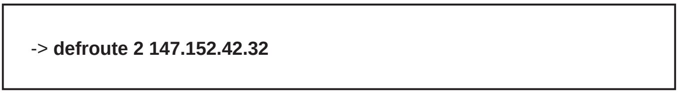
defroute [interface number] [IP address]

defroute delete [interface number] [IP address]

Description: The defroute command allows the user, in the syntax order shown above, to view, set, or delete the default IP route to a managed device through the specified interface.

Options: Not Applicable

Example:



```
-> defroute 2 147.152.42.32
```

05141-69

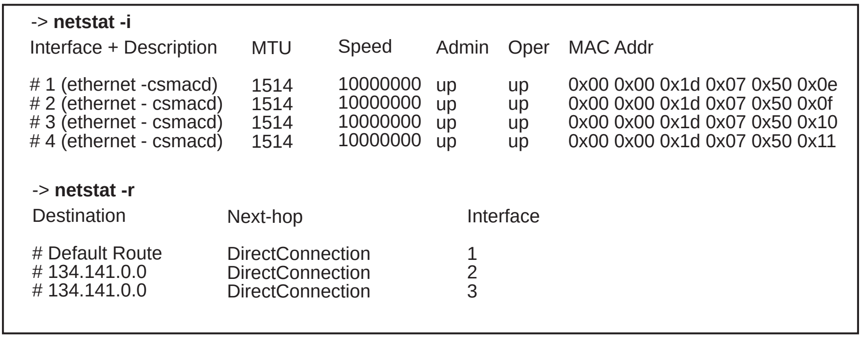
netstat:

Syntax: netstat [option]

Description: The netstat command provides a display of general network statistics for the managed device. The netstat command must be used with one of the two display options.

Options: -i Displays status and capability information for each interface.
-r Displays routing information for each interface.

Example:



```
-> netstat -i
Interface + Description    MTU     Speed      Admin   Oper    MAC Addr

# 1 (ethernet -csmacd)     1514    10000000   up      up      0x00 0x00 0x1d 0x07 0x50 0x0e
# 2 (ethernet - csmacd)    1514    10000000   up      up      0x00 0x00 0x1d 0x07 0x50 0x0f
# 3 (ethernet - csmacd)    1514    10000000   up      up      0x00 0x00 0x1d 0x07 0x50 0x10
# 4 (ethernet - csmacd)    1514    10000000   up      up      0x00 0x00 0x1d 0x07 0x50 0x11

-> netstat -r
Destination          Next-hop                  Interface

# Default Route      DirectConnection          1
# 134.141.0.0        DirectConnection          2
# 134.141.0.0        DirectConnection          3
```

05141-70

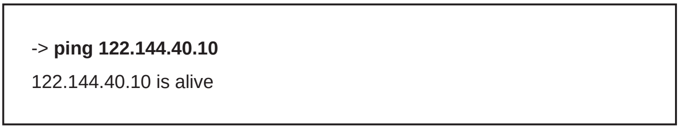
ping:

Syntax: ping [IP address]

Description: The ping command generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.

Options: Not Applicable

Example:



```
-> ping 122.144.40.10
122.144.40.10 is alive
```

05141-71

reset:

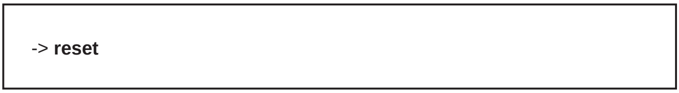
Syntax: reset

Description: This reset command initiates a hardware reset of the device.The reset command initializes the CPU processor, runs the onboard diagnostics, and restarts the software image, which restores the user configuration settings from NVRAM. The user will be queried to confirm the reset command to ensure against unwanted resets.

TIP The Network Tools connection to the device will be terminated upon execution of this command.

Options: Not Applicable

Example:



```
-> reset
```

17421-45

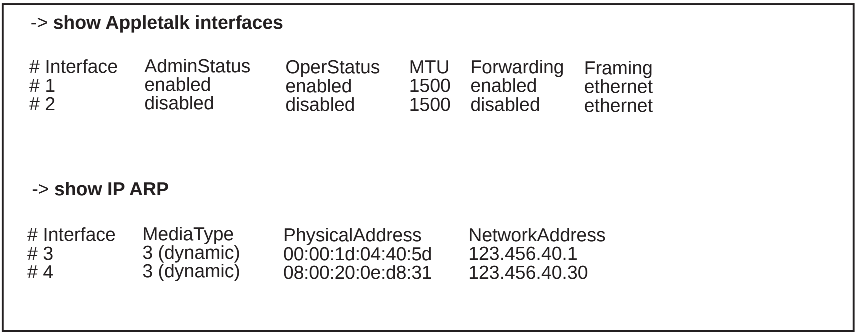
show:

Syntax: show <PROTOCOL> <TABLE>

Description: The show command displays information concerning various components of the device. Protocols currently supported are IP, IPX, DECnet, and AppleTalk. Components of those protocols that are currently supported are ARP caches, route tables, FIB tables, server tables, and interface tables. The number of valid entries in the table will be displayed at the end of the table display.

Options: Not Applicable

Example:



```
-> show Appletalk interfaces

# Interface    AdminStatus   OperStatus   MTU    Forwarding   Framing
# 1            enabled       enabled      1500   enabled      ethernet
# 2            disabled      disabled     1500   disabled     ethernet


-> show IP ARP

# Interface    MediaType     PhysicalAddress       NetworkAddress
# 3            3 (dynamic)   00:00:1d:04:40:5d     123.456.40.1
# 4            3 (dynamic)   08:00:20:0e:d8:31     123.456.40.30
```

17421-46

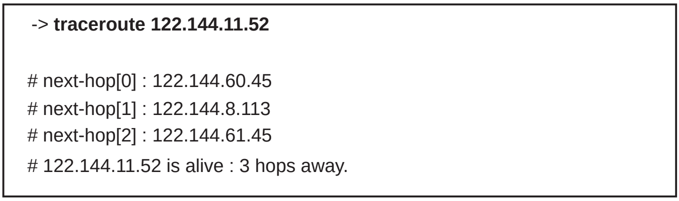
traceroute:

Syntax: traceroute [IP address]

Description: The traceroute command generates a TRACEROUTE request to a specified IP address and provides a display of all next-hop routers in the path to the device. If the device is not reached, the command displays all next-hop routers to the point of failure.

Options: Not Applicable

Example:



```
 -> traceroute 122.144.11.52

# next-hop[0] : 122.144.60.45
# next-hop[1] : 122.144.8.113
# next-hop[2] : 122.144.61.45
# 122.144.11.52 is alive : 3 hops away.
```

05141-77

soft_reset:

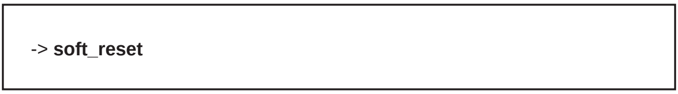
Syntax: soft-reset

Description: This command restarts the software image, which restores the user configuration settings from NVRAM. The user will be queried to confirm the reset command to ensure against unwanted resets.

TIP The Network Tools connection to the device will be terminated upon execution of this command.

Options: Not Applicable

Example:



```
-> soft_reset
```

22511-76

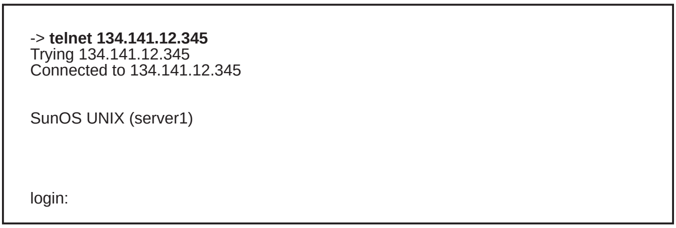
telnet:

Syntax: telnet [IP address] [Port #]

Description: The telnet command allows the user to communicate with another host (that supports Telnet connections) using the Telnet protocol. The user must specify the remote host using its IP address. The [IP address] field is mandatory. If no Port number is specified, telnet will attempt to contact the host at the default port.

Options: Not Applicable

Example:



```
-> telnet 134.141.12.345
Trying 134.141.12.345
Connected to 134.141.12.345


SunOS UNIX (server1)




login:
```

2251-77

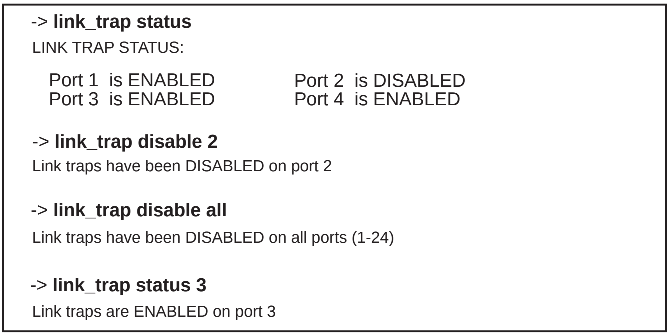
link_trap:

Syntax: link_trap [enable/disable/status] [PORT/all]

Description: The link_trap command allows link traps to be enabled or disabled when specifying a single port, or simultaneously when specifying “all” or no ports. When one or all ports are specified to enable, disable, or find their status, their current condition is displayed.

Options: Not Applicable

Example:



```
-> link_trap status
LINK TRAP STATUS:

   Port 1  is ENABLED              Port 2  is DISABLED
   Port 3  is ENABLED              Port 4  is ENABLED

-> link_trap disable 2
Link traps have been DISABLED on port 2

-> link_trap disable all
Link traps have been DISABLED on all ports (1-24)

-> link_trap status 3
Link traps are ENABLED on port 3
```

2314-78

atm_stp_state:

NOTE

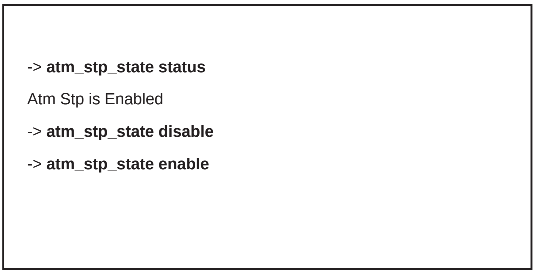
The **atm_stp_state** command is only available if an HSIM-A6DP is installed in the device (e.g., 6E13X-25). This command allows the user to enable, disable, or check the current status of the Spanning Tree Algorithm on all ATM interfaces.

Syntax: atm_stp_state [STATE]

Description: The atm_stp_state command allows the user to enable, disable, or check the status of the Spanning Tree Algorithm on all ATM interfaces. The user must specify the STATE option as enable, disable, or status. The STATE field is mandatory.

Options: enable, disable, status

Example:



```
-> atm_stp_state status
Atm Stp is Enabled
-> atm_stp_state disable
-> atm_stp_state enable
```

2314-79

5.35.2 Special Commands

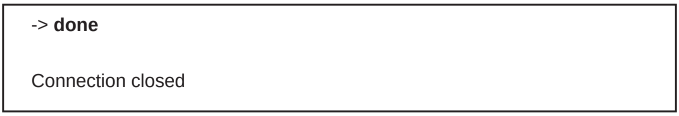
done, quit, exit:

Syntax: done, quit, or exit

Description: The done, quit, or exit command enables the user to exit from Network Tools and return to the Main Menu screen.

Options: Not Applicable

Example:



```
-> done

Connection closed
```

05141-72

APPENDIX A
SPECIFICATIONS

This appendix provides operating specifications for the Cabletron Systems 6H123-50 and 6H133-37 Interface Modules. Cabletron Systems reserves the right to change these specifications at any time without notice.

A.1 DEVICE SPECIFICATIONS

Processor:	Intel i960 RISC processor control
Dynamic Random Access Memory (DRAM):	20 MB
FLASH Memory:	4 MB

A.2 PHYSICAL PROPERTIES

Dimensions:	46.43 H x 6.05 W x 32.39 D (cm) 18.28 H x 2.38 W x 12.75 D (in)
Weight (Unit):	2.72 kg (6 lb)
MTBF (Predicted):	200,000 hours

A.3 ENVIRONMENTAL REQUIREMENTS

Operating Temperature:	5° to 40°C (41° to 104°F)
Storage Temperature:	-30° to 73°C (-22° to 164°F)
Operating Relative Humidity:	5% to 90% (non-condensing)

A.4 INPUT/OUTPUT PORTS

6H123-50

CONN 1 through 4	Ethernet (10BASE-T/100BASE-TX compliant) with RJ21 type connectors.
Slots for optional Fast Ethernet Interface Modules (slots 5 and 6)	Slots accept three types of optional Fast Ethernet Interface Modules: the FE100-TX, FE100-FX and the FE-100F3.

6H133-37

CONN 1 through 3	Ethernet (10BASE-T/100BASE-TX compliant) with RJ21 type connectors.
Slot for optional HSIM	Slot accepts optional High Speed Interface Module (HSIM).

A.5 COM PORT PINOUT ASSIGNMENTS

The COM port is a serial communications port that supports Local Management or connection to a UPS.

The COM port has the following pin assignments:

Table A-1 COM Port Pin Assignments

Pin	Signal Name	Input/Output
1	Transmit Data (XMT)	Output
2	Data Carrier Detect (DCD)	Output
3	Data Set Ready (DSR)	Input
4	Receive Data (RCV)	Input
5	Signal Ground (GND)	NA
6	Data Terminal Ready (DTR)	Output
7	Request to Send (RTS)	Input
8	Clear to Send (CTS)	NA

A.6 REGULATORY COMPLIANCE

This equipment meets the following safety and electromagnetic compatibility (EMC) requirements:

Safety	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 73/23/EEC.
EMC	FCC Part 15, EN 55022, CSA C108.8, EN 50082-1, AS/NZS 3548, VCCI V-3, and 89/336/EEC.

APPENDIX B

FE-100TX, FE-100FX AND FE-100F3 SPECIFICATIONS

The 6H123-50 and the 6H133-37 support three Fast Ethernet Interface Modules:

- FE-100TX
- FE-100FX
- FE-100F3

This appendix provides the specifications for these modules.

B.1 FE-100TX

The FE-100TX uses an RJ45 connector supporting Category 5 Unshielded Twisted Pair (UTP) cabling.

NOTE

To ensure proper operation, use only Category 5 Unshielded Twisted Pair (UTP) cabling that has an impedance between 85 and 111 ohms.

The slide switch on the FE-100TX determines the crossover status of the cable pairs. If the switch is on the **X** side, the pairs are internally crossed over. If the switch is on the **=** side, the pairs are not internally crossed over. Figure B-1 shows the pinouts for the FE-100TX in both positions.

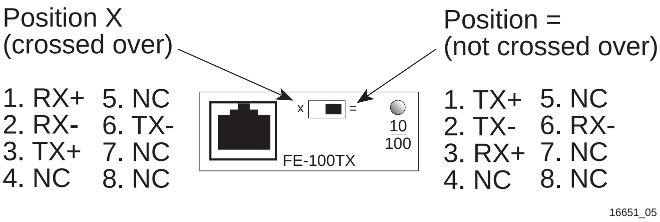


Figure B-1 FE-100TX RJ45 Pinouts

B.2 FE-100FX

The FE-100FX shown in Figure B-2 uses an SC style connector that supports multimode fiber optic cabling. Specifications for the FE-100FX are listed below.

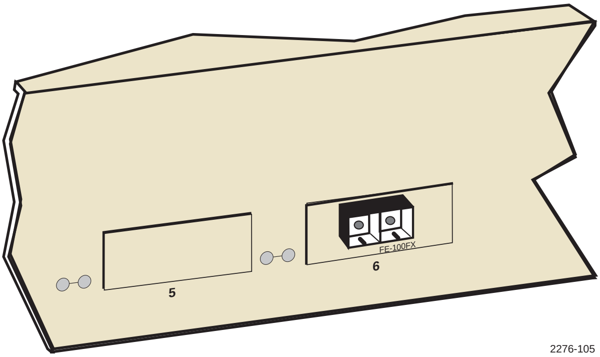


Figure B-2 FE-100FX

Table B-1 Transmitter Power

Cable Type	Worst Case Budget	Typical Budget
50/125 µm fiber	6.0 dB	9.0 dB
62.5/125 µm fiber	9.0 dB	12.0 dB
100/140 µm fiber	15.0 dB	18.0 dB

NOTE

The transmitter power levels and receive sensitivity levels listed are peak power levels after optical overshoot. A peak power meter must be used to correctly compare the values given above to those measured on any particular port. If power levels are being measured with an average power meter, add 3 dB to the measurement to compare the measured values to the values listed above.

B.3 FE-100F3

The FE-100F3 shown in Figure B-3 uses an SC style connector that supports single mode fiber optic cabling. Specifications for the FE-100F3 are listed in Table B-2 below.

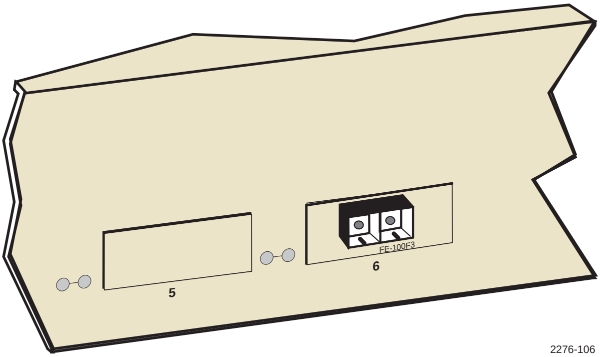


Figure B-3 FE-100F3

Table B-2 Transmitter Power

Cable Type	Worst Case Budget	Typical Budget
8/125 µm fiber	>10.0 dB	<10.0 dB
12/125 µm fiber	>10.0 dB	<10.0 dB

NOTE

The transmitter power levels and receive sensitivity levels listed are peak power levels after optical overshoot. A peak power meter must be used to correctly compare the values given above to those measured on any particular port. If power levels are being measured with an average power meter, add 3 dB to the measurement to compare the measured values to the values listed above.

APPENDIX C

OPTIONAL INSTALLATIONS AND MODE SWITCH BANK SETTINGS

ONLY QUALIFIED SERVICE PERSONNEL SHOULD ATTEMPT THE FOLLOWING PROCEDURES.

NUR QUALIFIEZIERTE SERVICE PERSONNAL DIE FOLGENDE PROCEDURE FOLGEN SOLLTEN.

SOLAMENTE PERSONAL CALIFICADO DEBE INTENTAR ESTE PROCEDIMIENTO.

This appendix covers the following items:

- Required tools (Section C.1)
- Locations, functions, and settings for the mode switches (Section C.2)
- Installing Optional Fast Ethernet Interface Modules (Section C.3)

C.1 REQUIRED TOOLS

The following tools are required to perform the procedures provided in this appendix:

- Antistatic wrist strap (provided with the 6C105 chassis)
- Phillips screwdriver

C.2 SETTING THE MODE SWITCHES

These switches are set at the factory and do not need to be changed unless you intend to perform the following:

- Force download a new image file from a BootP server.
- Clear NVRAM and restore all user-entered parameters such as the IP address and subnet mask to the 6H123-50 and 6H133-37 “Default” configuration settings.
- Clear user-entered passwords stored in NVRAM and restore the default passwords.

Figure C-1 shows the location of the mode switches and the switch settings for normal operation.

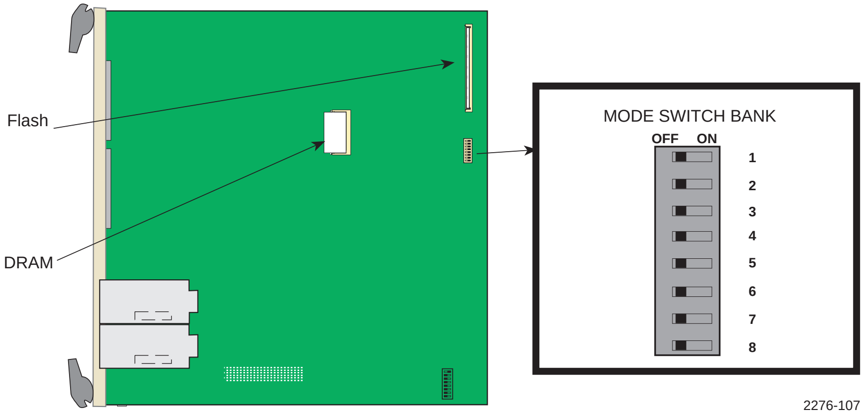


Figure C-1 6H123-50 AND 6H133-37 Mode Switch Location/Component Layout

Switch definitions and positions are as follows:

- Switches 1 through 4 – For Cabletron Systems use only.
- Switch 5 – COM Port Autobaud. The default (OFF) position enables Autobaud sensing on the COM port for Local Management sessions. Changing the switch to the ON position disables Autobaud sensing and sets the COM port to 9600 baud for Local Management sessions.
- Switch 6 – Forced BootP. Changing the position of this switch (i.e., moving the switch from one position to the other) clears download information from NVRAM and forces the 6H123-50 and 6H133-37 to download a new image file from a BootP server after power to the chassis is restored or the reset button is pressed.

NOTE

After changing the position of switch 6, DO NOT reapply power to the chassis or reset the module until there is a station acting as a BootP server, which contains the image file.

- After changing the position of switch 6 and restarting the module, the 6H123-50 and 6H133-37 request a new image download until they either receive a new image or the RESET button on the front panel is pressed. When the RESET button is pressed, the 6H123-50 and 6H133-37 continue trying to contact a BootP server, but will time out in approximately one minute. If the module times out, the image is downloaded from its FLASH memory.
- Switch 7 – Clear NVRAM. Changing the position of this switch resets NVRAM on the next power up. ALL user entered parameters, such as IP addresses, subnet mask, SNMP traps, and bridging functions are restored to their factory default settings.
- Switch 8 – Reset Password/Community Strings. Changing the position of this switch clears only the user-entered passwords stored in NVRAM, and restores the default passwords. Once the 6H133-37 or 6H123-50 is reset, the passwords can either be reentered or the default passwords (Public and ENTER) may be used.

NOTE

Do not change the position of switch 8 unless it is necessary to reset the module super-user configured passwords to their factory default settings.

C.3 INSTALLING OPTIONAL FAST ETHERNET INTERFACE MODULES

Figure C-2 shows the location of the Fast Ethernet Interface Module connectors on the 6H123-50 boards for slots 5 and 6.

NOTE

For instructions on installing a High Speed Interface Module (HSIM) in the 6H133-37 refer to the applicable HSIM documentation.

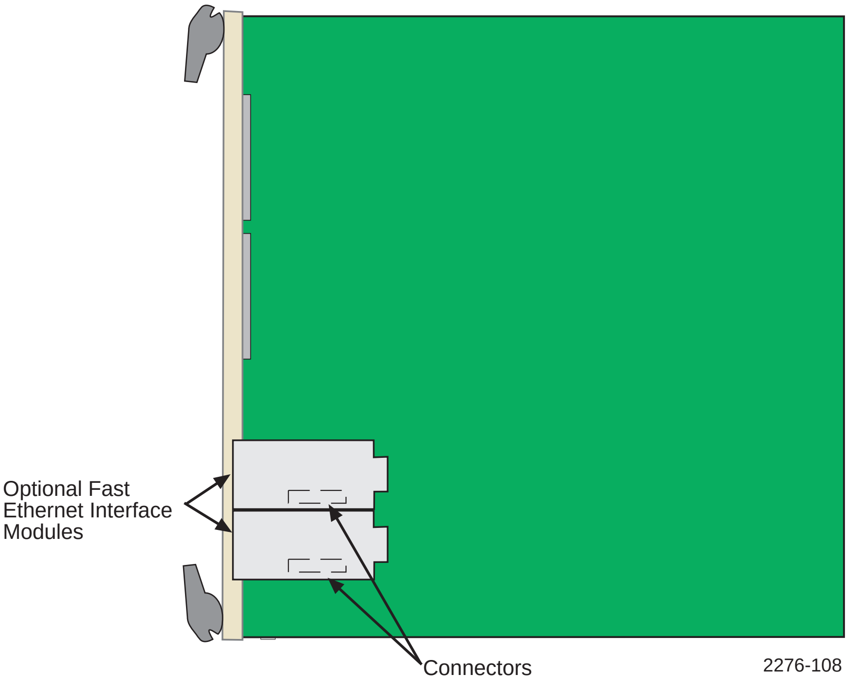


Figure C-2 6H123-50 Fast Ethernet Interface Module Connector Location

To install a Fast Ethernet Interface Module in port slot 5 or 6 of the 6H123-50, proceed as follows:

! CAUTION

The Fast Ethernet Interface Module and the host module are sensitive to static discharges. Use an antistatic wrist strap and observe all static precautions during this procedure. Failure to do so could damage the Fast Ethernet Interface Module or the host module.

! CAUTION

The FE-100F3 uses Class 1 lasers. Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, remove power from the network adapter.

1. Remove the coverplate from the port slot where the Fast Ethernet Interface Module will be installed.

TIP

When installing Fast Ethernet Interface Modules in both slots 5 and 6, remove the coverplates from both slot openings. In the following instructions, the optional module is shown being installed in port slot 6.

To remove a coverplate, refer to Figure C-3 and proceed as follows:

a. Remove the two screws fastening the coverplate to the standoffs. Save the screws.

b. Lift and remove the coverplate from the top of the front standoffs.

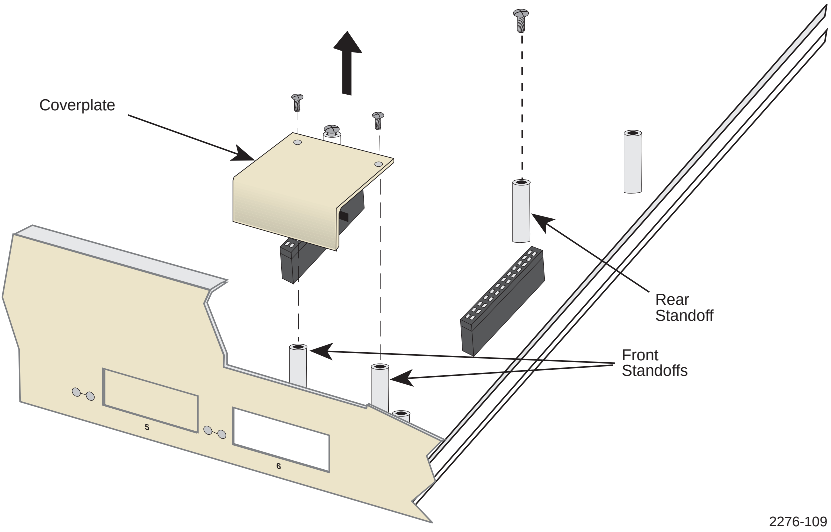


Figure C-3 Coverplate Removal

2. Remove the screw from the rear standoff. Save the screw.

CAUTION When installing an FE-100FX or FE-100F3 module into the host module, remove the rubber plug on the SC connector before proceeding.

3. See Figure C-4. Gently pull the faceplate of the host module forward to allow room for the Fast Ethernet Interface Modules to be aligned over the connector.

4. Carefully lower the Fast Ethernet Interface Module onto the standoffs while inserting the module connector into the associated motherboard connector.

CAUTION

When inserting the Fast Ethernet Interface Module into the motherboard connector ensure that the pins do not bend, as this can damage both the Fast Ethernet Interface Module and the motherboard connector.

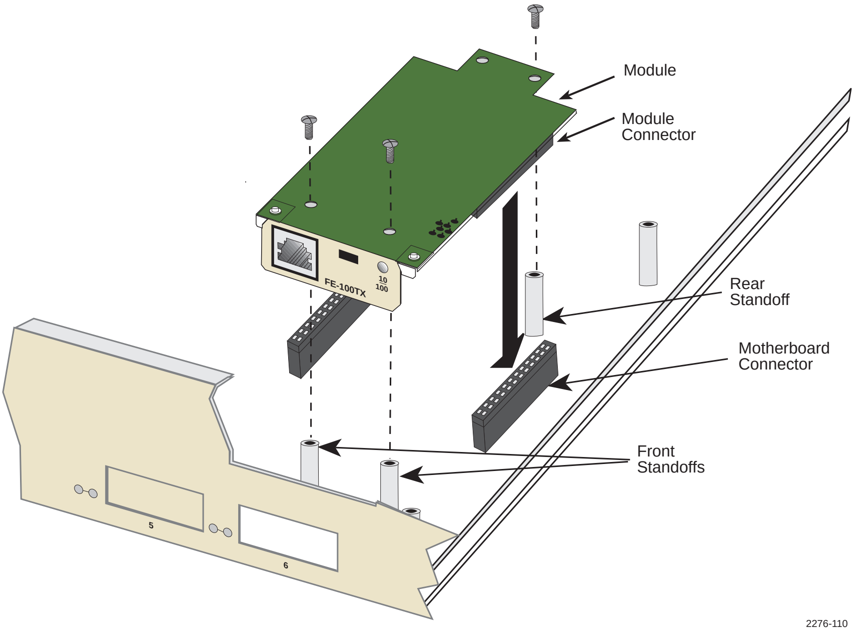


Figure C-4 Installing the Fast Ethernet Interface Module

5. Press down firmly on the Fast Ethernet Interface Module until the pins slide all the way into the motherboard connector. Ensure that the Fast Ethernet Interface Module seats flush on the standoffs.

6. Secure the Fast Ethernet Interface Module with the screws saved in steps 1 and 2.

INDEX